Relatively Free Algebras with the Identity $x^3 = 0$

A. A. Lopatin
Chair of Algebra,
Department of Mathematics,
Omsk State University,
55A Prospect Mira, Omsk 644077, Russia,
e-mail: lopatin@math.omsu.omskreg.ru

Abstract

A basis for a relatively free associative algebra with the identity $x^3 = 0$ over a field of an arbitrary characteristic is found. As an application, a minimal generating system for the 3×3 matrix invariant algebra is determined.

1 Introduction

Let K be an infinite field of an arbitrary characteristic p ($p = 0, 2, 3, \ldots$). Let $K\langle x_1, \ldots, x_d\rangle^{\#}$ ($K\langle x_1, \ldots, x_d\rangle$, respectively) be the free associative K-algebra without unity (with unity, respectively) which is freely generated by $x_1, \ldots, x_d$. Let $\mathrm{id}\{f_1, \ldots, f_s\}$ be the ideal generated by $f_1, \ldots, f_s$. Denote by $N_{n,d} = K\langle x_1, \ldots, x_d\rangle^{\#}/\ \mathrm{id}\{x^n | x \in K\langle x_1, \ldots, x_d\rangle^{\#}\}$ a relatively free finitely generated non-unitary K-algebra with the identity $x^n = 0$, where $d \geq 1$. Let $\mathcal{N} = \{0, 1, 2, \ldots\}$. The algebra $N_{n,d}$ possesses natural $\mathcal{N}$- and $\mathcal{N}^d$-gradings by degrees and multidegrees respectively.

The *nilpotency degree* of a non-unitary algebra A is the least $C > 0$ for which $a_1 \cdots a_C = 0$ for all $a_1, \ldots, a_C \in A$. Denote by $C(n, d, K)$ the nilpotency degree of $N_{n,d}$. In the case of characteristic zero $n(n+1)/2 \leq C(n, d, K) \leq n^2$ (see [8], [11]), and there is a conjecture that $C(n, d, K) = n(n+1)/2$. This conjecture has been proven for $n \leq 4$ (see [13]). If $p = 0$ or $p > n$, then $C(n, d, K) < 2^n$ by [6]. For a positive characteristic some upper bounds on $C(n, d, K)$ are given in [7]: $C(n, d, K) < (1/6)n^6 d^n$ and $C(n, d, K) < 1/(m-1)!\, n^{n^3} d^m$, where $m = [n/2]$.

In [9] $C(3,d,K)$ was established for an arbitrary d,p, except for the case of $p=3$, d is odd, where the deviation in the estimation of $C(3,d,K)$ is equal to 1. In this article, a basis for $N_{3,d}$ is found (see Proposition 2 and Theorems 2, 3), and, in particular, $C(3,d,K)$ is established for any d,p. Namely, when $d>1$, we have:

$$\begin{array}{l}
\text{If } p=0 \text{ or } p>3, \text{ then } C(3,d,K)=6.\\
\text{If p=2, then } C(3,d,K)=\left\{\begin{array}{lcl} d+3 & , & d\geq 3\\ 6 & , & d=2.\end{array}\right.\\
\text{If } p=3, \text{ then } C(3,d,K)=3d+1.
\end{array}$$

As an application, a minimal homogeneous generating system of the 3×3 matrix invariant algebra is determined (see Theorem 4).

For $p=2,3$, a basis for the multilinear homogeneous component of $N_{3,d}$ for 'small' d was found by means of a computer programme. Then, the case of an arbitrary d was reduced to the case of 'small' d using the composition method. All programmes were written by means of Borland C++ Builder (version 6.0) and are available upon request from the author. The notion of the composition method was taken from [2].

2 Preliminaries

Further, we assume that $n=3$, unless it is stated otherwise. Let $\mathcal{Z}$ be the ring of integers, and let $\mathcal{Q}$ be the field of rational fractions. Denote by F_d the free semigroup, generated by letters $\{x_1,x_2,\ldots,x_d\}$. By $F_d^{\#}$ we mean F_d without unity. For short, we will write $K\langle F_d\rangle$ instead of $K\langle x_1,\ldots,x_d\rangle$. The degree of a $\mathcal{N}^d$-homogeneous element $u\in F_d$ we denote by $\deg(u)$, its multidegree we denote by $\mathrm{mdeg}(u)$, and the degree of u in letter x_j we denote by $\deg_{x_j}(u)$. Elements of F_d are called words. By words from $N_{3,d}$ we mean images of words from F_d in $N_{3,d}$ under the natural homomorphism. We assume that all words are non-empty, that is they are not equal to unity of F_d, unless it is stated otherwise. Notation $w=x_{i_1}\cdots\widetilde{x}_{i_s}\cdots x_{i_t}$ stands for the word w, which can be get from the word $x_{i_1}\cdots x_{i_t}$ by eliminating the letter x_{i_s}. For a set of words M and a word v denote by vM the set $\{vu|\,u\in M\}$. If the set M is empty, then we assume $vM=\emptyset$. By $x_i\cdots x_j$ $(i,j\in\mathcal{Z})$ we mean the word $x_ix_{i+1}x_{i+2}\cdots x_j$ if $1\leq i\leq j$, and the empty word otherwise.

For some $\mathcal{N}^d$-graded algebra A and multidegree $\Delta=(\delta_1,\ldots,\delta_d)$ denote by $A(\Delta)$ or $A(\delta_1,\ldots,\delta_d)$ the homogeneous component of A of multidegree Δ. For short, multidegree $(3,\ldots,3,2,\ldots,2,1\ldots,1)$ will be denoted by $3^r2^s1^t$ for the appropriate

r, s, t. For $\Delta = (\delta_1, \dots, \delta_t)$ let $|\Delta| = \sum_i \delta_i$. By $\operatorname{lin}\{v_1, \dots, v_t\}$ we mean the linear span of the elements $v_1, \dots, v_t$ of some vector space over K. We denote some elements of $K\langle F_d\rangle^\#$ by underlined Latin letters.

Endow the set of words of F_d with the partial lexicographical order. We put $x_{i_1}x_{i_2}\cdots x_{i_k} < x_{j_1}x_{j_2}\cdots x_{j_t}$ if we have $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$, $i_s < j_s$ for some $s \geq 1$. Note that if $v \in F_d^\#$, then words u and uv are incomparable.

By an *identity* we mean an element of $K\langle F_d\rangle$. All identities are assumed to be $\mathcal{N}^d$-homogeneous, unless the contrary is stated. The multidegree of an identity t we denote by $\operatorname{mdeg}(t)$. An identity t is said to be an identity of $N_{3,d}$, if the image of t in $N_{3,d}$ under the natural homomorphism is equal to zero. The zero polynomial is called the *trivial* identity.

For identity $f = \sum_i \alpha_i u_i$, $\alpha_i \in K$, $u_i \in F_d^\#$, $\overline{f}$ stands for the highest term of f, i.e., $\overline{f}$ is the maximal word from the set $\{u_i\}$. It is easy to see that, due to homogeneity, the highest term is unique. For a set of identities M, denote by $\overline{M}$ the set of the highest terms of the elements from M.

An identity is called *reduced* if the coefficient of its highest term is equal to 1.

We say that the identity is a *consequence* of a set of identities, provided it belongs to the linear span of these identities. As an example, we point out that x_1^3 is not a consequence of x_2^3.

An element $\sum_i \alpha_i u_i \in K\langle F_d\rangle$, where $\alpha_i \in K$, $u_i \in F_d^\#$, is called *an element generated by words* $v_1, \dots, v_t$, if all u_i are products of some elements from $\{v_1, \dots, v_t\}$.

For identities t_1, t_2 and for a set of identities M, notation $t_1 = t_2 + \{M\}$ means that $t_1 \in t_2 + \operatorname{lin} M$.

Consider an element $g \in K\langle F_d\rangle$ and an identity $t = u + (\sum_{i=1}^r \alpha_i u_i)$, where $\alpha_i \in K$, $u, u_1, \dots, u_r$ are pairwise different words. Let $g_1 = g$. If $g_k = v_1 u v_2 + \sum_{j=1}^s \beta_j w_j$ for pairwise different words $v_1 u v_2, w_1, \dots, w_s$ and $\beta_j \in K$, then $g_{k+1} = -\sum_{i=1}^r \alpha_i v_1 u_i v_2 + \sum_{j=1}^s \beta_j w_j$. Note that g_{k+1} is not uniquely determined by g_k and t. If there is k such that $g_k = \sum_{j=1}^s \beta_j w_j$ for some words $w_1, \dots, w_s$ which do not contain subword u, then we say that the chain $g_1, \dots, g_k$ is finite and g_k is its result. If every chain is finite and they all have one and the same result g', then we call the identity g' *the result of application* of the identity t with the *marked word* u to the identity g. Otherwise we say that the result of application of t with the marked word u to g is indefinite.

The result of substitution $v_1 \to u_1, \dots, v_k \to u_k$ in $f \in K\langle F_d\rangle$, where f is an element generated by words $v_1, \dots, v_k, v_{k+1}, \dots, v_t$, denote by $f|_{v_1 \to u_1, \dots, v_k \to u_k}$. By *substitutional mapping* we mean such homomorphism of K-algebras $\phi : K\langle F_k\rangle \to K\langle F_l\rangle$ that $\phi(x_i) \in F_l^\#$, $i = \overline{1,k}$. A substitutional mapping is called monotonous, if

$\phi(x_i) > \phi(x_j)$ for $x_i > x_j$. The set of monotonous substitutional mappings denote by $\mathcal{M}_{k,l}$. Note that for $\phi \in \mathcal{M}_{i,j}$, $\psi \in \mathcal{M}_{j,k}$ the composition $\psi \circ \phi$ belongs to $\mathcal{M}_{i,k}$.

Denote

$$T_1(a) = a^3,$$

$$T_2(a,b) = a^2b + aba + ba^2,$$

$$T_3(a,b,c) = abc + acb + bac + bca + cab + cba.$$

Partial and complete linearization of the identity $f_1a^3f_2$ of $N_{3,d}$, where $a \in K\langle F_d\rangle^{\#}$, $f_1, f_2 \in F_d$, gives that all identities from $\mathcal{S} = \{f_1T_1(a)f_2,\ f_1T_2(a,b)f_2,\ f_1T_3(a,b,c)f_2|\ a,b,c \in F_d^{\#},\ f_1,f_2 \in F_d\}$ are identities of $N_{3,d}$. For multidegree Δ let $\mathcal{S}_\Delta$ be the subset of $\mathcal{S}$ which consists of all identities of multidegree Δ. Clearly, each identity of $N_{3,d}(\Delta)$ is a consequence of the set of identities $\mathcal{S}_\Delta$. The set of identities $\mathcal{S}_\Delta$ can be treated like the system of homogeneous linear equations in formal variables $\{w|w \in F_d^{\#}, \mathrm{mdeg}(w) = \Delta\}$. Then, free variables of the system $\mathcal{S}_\Delta$ form a basis for $N_{3,d}(\Delta)$. We call two systems of linear equations (two sets of identities, respectively) equivalent, if the first one is a consequence of the second and vice versa.

A word $w \in S$ is called *canonical* with respect to x_i, if it has one of the following forms: w_1, $w_1x_iw_2$, $w_1x_i^2w_2$, $w_1x_i^2ux_iw_2$, where words w_1, w_2, u do not contain x_i, words w_1, w_2 can be empty. If a word is canonical with respect to all letters, then we call it *canonical*. Number for future references the identity of $N_{3,d}$

$$xux + (x^2u + ux^2),\ u \in F_d^{\#}. \tag{1}$$

3 Auxiliary results

We will use the following facts from [9]:

Lemma 1 *1. Applying identities (1), $x_iux_i^2 = -x_i^2ux_i$ of $N_{3,d}$, any non-zero word $w \in N_{3,d}$ can be represented as a sum of canonical words which belong to the same homogeneous component as w. In particular, if $\deg_{x_i}(w) > 3$, $w \in F_d$, then $w = 0$ in $N_{3,d}$.*

2. The inequality $x_1^2x_2^2x_1 \neq 0$ holds in $N_{3,d}$.

3. If $p = 0$ or $p > 3$, then $C(3,d,K) = 6$ $(d \geq 2)$.
If $p = 2$, then $C(3,d,K) = d+3$, where $d \geq 3$, and $C(3,2,K) = 6$.

4. If $p \neq 3$, then $x^2ay^2 = 0$ is an identity of $N_{3,d}$, where $a \in F_d^{\#}$.

5. If $p = 3$, then $x^2y^2xay = x^2y^2xya$ is an identity of $N_{3,d}$, where $a \in F_d^{\#}$.

6. If $p=2$, then $x_1^2x_2\cdots x_dx_1\neq 0$ holds in $N_{3,d}$.

7. If $p\neq 3$, then $I_1(x,a,b,c)=x^2abc+x^2acb$, $I_2(x,a,b,c)=abcx^2+bacx^2$, $I_3(x,a,b,c)=ax^2bc+cax^2b$ are identities of $N_{3,d}$, where x, a, b, c are words.

Proof. 1. See [9], Statement 1.

2. See [9], Statement 3.

3. See [9], Propositions 1, 2.

4. See [9], equality (5).

5. See [9], proof of Statement 7.

6. See [9], Statement 4.

7. Let x,a,b,c be words, $p\neq 3$. Partial linearization of the identity from item 4 with respect to x (y, respectively) gives that $I_1(x,a,b,c)$, $I_2(x,a,b,c)$ are identities of $N_{3,d}$. Apply identity (1), where $x=x_1$, to the identity $T_3(x_1a,bx_1,c)=0$ of $N_{3,d}$, and get that $-T_3(x_1^2a,b,c)-T_3(a,bx_1^2,c)+3(bx_1^2ac+cbx_1^2a)=0$ in $N_{3,d}$. Hence $I_3(x,a,b,c)$ is the identity of $N_{3,d}$. $\triangle$

Remark 1 *1. Consider a set $M=\{m_i\}_{i=\overline{1,s}}\subset K\langle F_d\rangle^{\#}$. Let $u\in F_d^{\#}$ be a word which is a summand of one and only one element m_1 of the set M. Let $\sum_{i=1}^{s}\alpha_im_i=0$ in $K\langle F_d\rangle$, where $\alpha_i\in K$. Then $\alpha_1=0$.*

2. Let Δ be a multidegree. Let $V=\{v_1,\dots,v_s\}$ be a set of words of multidegree Δ. Assume that for each word w, of multidegree Δ, which do not lie in V there is an identity $w-f_w$ of $N_{3,d}$, where $f_w\in\operatorname{lin}V$. Then every identity $\sum_i\alpha_iv_i$ ($\alpha_i\in K$) of $N_{3,d}(\Delta)$ is a consequence of the identities which are results of application of identities $\{w-f_w\}$ to the identities of $\mathcal{S}_\Delta$. (Note that results of these applications are defined.)

Lemma 2 *Let $d\geq 1$. All identities, of $N_{3,d}(21^{d-1})$, generated by $x_1^2,x_2,\dots,x_d$ are consequences of the following identities of $N_{3,d}(21^{d-1})$:*

(a) $f_1T_3(a,b,c)f_2$, where some word from a, b, c, f_1, f_2 contains the subword x_1^2,

(b) $3f_1I_i(x_1,a,b,c)f_2$, $i=\overline{1,3}$.

Here $a,b,c\in F_d^{\#}$, $f_1,f_2\in F_d$.

Proof. By item 2 of Remark 1, any identity, of $N_{3,d}(21^{d-1})$, generated by $x_1^2,x_2,\dots,x_d$ is a consequence of identities which are results of application of identity (1) (where $x=x_1$) to the identities from $\mathcal{S}_{21^{d-1}}$.

If we apply (1), where $x=x_1$, to $T_2(x_1,a)=0$, then we get a trivial identity.

The result of application of (1), where $x=x_1$, to an identity $t=f_1T_3(a_1,a_2,a_3)f_2$, where $a_1,a_2,a_3\in F_d^{\#}$, $f_1,f_2\in F_d$, denote by t', and let $t=\sum_{i=1}^{6}u_i$ for some words $u_1,\dots,u_6$. If words $u_1,\dots,u_6$ do not contain subword x_1^2 and $a_i\neq x_1$, $i=\overline{1,3}$, then t' is a consequence of identities (a). Let $a,b,c\in F_d^{\#}$.

If $t = T_3(x_1, x_1, a)$, then $t' = 0$.
If $t = T_3(x_1a, x_1, b)$, then $t' = -T_3(x_1^2, a, b)$.
If $t = T_3(ax_1b, x_1, c)$, then $t' = -T_3(ab, x_1^2, c) - 3I_3(x_1, a, b, c)$.
If $t = T_3(x_1a, bx_1, c)$, then $t' = -T_3(x_1^2a, b, c) - T_3(a, bx_1^2, c) + 3I_3(x_1, b, a, c)$.
If $t = x_1aT_3(x_1, b, c)$, then $t' = -aT_3(x_1^2, b, c) - 3I_1(x_1, a, b, c)$.
If $t = x_1T_3(x_1, a, b)$, then $t' = -T_3(x_1^2, a, b)$.
If $t = x_1T_3(x_1a, b, c)$, then $t' = -x_1^2T_3(a, b, c) - T_3(x_1^2a, b, c) + 3I_1(x_1, a, b, c)$.

Due to the fact that, if we read identities (a), (b) from right to left, they do not change, the claim follows from the regarded cases. $\triangle$

Let $r = \overline{1,d}$. It is easy to see that for every $i = \overline{1,r}$ the result of application of the identity (1), where $x = x_i$, to every identity of multidegree 2^r1^{d-r} is definite. For $\sigma \in S_r$ let $\psi_\sigma : K\langle F_d\rangle(2^r1^{d-r}) \to K\langle F_d\rangle(2^r1^{d-r})$ be such mapping that $\psi_\sigma(t)$ is the result of the following procedure. Let t_1 be the result of application of the identity (1), where $x = x_{\sigma(1)}$, to t. For $i = \overline{2,r}$ let t_i be the result of application of the identitiy (1), where $x = x_{\sigma(i)}$, to t_{i-1}. We define $\psi_\sigma(t) = t_r$.

For any identity $t = \sum_{i=1}^s \alpha_i u_i$, $\alpha_i \in K$, $u_i \in F_d^{\#}$, of multidegree 2^r1^{d-r}, fix some permutations $\sigma_{t,1}, \dots, \sigma_{t,s} \in S_r$. Consider the mapping $\psi : K\langle F_d\rangle(2^r1^{d-r}) \to K\langle F_d\rangle(2^r1^{d-r})$ such that for $t = \sum_i \alpha_i u_i$, $\alpha_i \in K$, $u_i \in F_d^{\#}$, we have $\psi(t) = \sum_i \alpha_i \psi_{\sigma_{t,i}}(u_i)$. Denote by Ψ_r the set of all such mappings ψ.

Lemma 3 *Let $d, r \geq 1$, $\phi \in \Psi_r$. All identities, of $N_{3,d}(2^r1^{d-r})$, generated by $x_1^2, \dots, x_r^2$, $x_{r+1}, \dots, x_d$ are consequences of the following identities of $N_{3,d}(2^r1^{d-r})$:*

(a) $f_1T_3(a, b, c)f_2$, where for each $k = \overline{1,r}$ some word from a, b, c, f_1, f_2 contains the subword x_k^2,

(b) $3\phi(f_1I_i(x_k, a, b, c)f_2)$, $i = \overline{1,3}$, $k = \overline{1,r}$,

(c) the identity $3f_1x_i^2ax_j^2f_2$ ($i, j = \overline{1,r}$, $i \neq j$) which is generated by $x_1^2, \dots, x_r^2$, $x_{r+1}, \dots, x_d$.
Here $a, b, c \in F_d^{\#}$, $f_1, f_2 \in F_d$.

Proof. For $\psi \in \Psi_r$ denote the sets of identities of multidegree 2^r1^{d-r}: $A_1 = \{\psi_\sigma(w) - \psi_\tau(w) \mid w \in F_d,\ \sigma, \tau \in S_r\}$, $A_2^\psi = \{\psi(t) \mid t = f_1T_2(a, b)f_2,\ a, b \in F_d^{\#},\ f_1, f_2 \in F_d\}$ and $A_3^\psi = \{\psi(t) \mid t = f_1T_3(a, b, c)f_2,\ a, b, c \in F_d^{\#},\ f_1, f_2 \in F_d\}$.

For an arbitrary $\psi \in \Psi_r$ identities, of $N_{3,d}(2^r1^{d-r})$, generated by $x_1^2, \dots, x_r^2$, $x_{r+1}, \dots, x_d$ are consequences of A_1, A_2^ψ, A_3^ψ (see item 2 of Remark 1). The following items conclude the proof.

1. *Identities A_1 are consequences of identities (c). In particular, $\psi(t) = \pi(t) + \{(a), (b), (c)\}$ and $\psi(t + f) = \psi(t) + \psi(f)$ for any $\psi, \pi \in \Psi_r$, $t, f \in K\langle F_d\rangle(2^r1^{d-r})$.*

Proof. Note that the identity $\psi(3f_1x_i^2ax_j^2f_2) \in K\langle F_d\rangle(2^r1^{d-r})$, where $a \in F_d^{\#}$, follows from (c).

If $r = 1$ then $A_1 = \{0\}$. Let $r = 2$. Denote $\psi_1(w) = \psi_\sigma(w) - \psi_\tau(w)$, where $\sigma = 1 \in S_2$, $\tau = (1,2) \in S_2$. If $w = x_1ax_1bx_2cx_2$ or $w = x_1ax_2bx_2cx_1$, $a, b, c \in F_d$, then the identity $\psi_1(w)$ is trivial. Consider $w = x_1ax_2bx_1cx_2$, $a, b, c \in F_d$. Then $\psi_1(w) = (x_1ax_2bx_1)cx_2 - x_1a(x_2bx_1cx_2)$ in $N_{3,d}$, where the order of application of identity (1) is determined by parentheses.

If $ab, bc \neq 1$, then $\psi_1(w) = (-x_1^2ax_2bcx_2 - ax_2bx_1^2cx_2) - (-x_1ax_2^2bx_1c - x_1abx_1cx_2^2) = (x_1^2ax_2^2bc + x_1^2abcx_2^2 + ax_2^2bx_1^2c + abx_1^2cx_2^2) - (x_1^2ax_2^2bc + ax_2^2bx_1^2c + x_1^2abcx_2^2 + abx_1^2cx_2^2) = 0$.

If $a = b = c = 1$, then $\psi_1(w) = 0$.

If $a = b = 1$, $c \neq 1$, then $\psi_1(w) = 3x_1^2cx_2^2$.

If $b = c = 1$, $a \neq 1$, then $\psi_1(w) = -3x_1^2ax_2^2$.

Therefore, if $r = 2$ then the required is proved.

The case of $r > 2$ follows from the case of $r = 2$ and the fact that any permutation is a composition of elementary transpositions.

2. *Identities A_3^ψ are consequences of identities* (a), (b), (c).

Proof. It follows from Lemma 2 and item 1.

3. *Identities A_2^ψ are consequences of identities* (a), (b), (c).

Proof. We will use item 1 without reference. Prove by induction on k that for every identity $t = f_1T_2(v,a)f_2$ of multidegree 2^r1^{d-r} we have $\psi(t) = 0 + \{(a),(b),(c)\}$, i.e., $\psi(f_1 \cdot vav \cdot f_2) = -\psi(f_1 \cdot v^2a \cdot f_2) - \psi(f_1 \cdot av^2 \cdot f_2) + \{(a),(b),(c)\}$, where $v, a \in F_d^{\#}$, $f_1, f_2 \in F_d$, and $\deg(v) = k$.

Induction base is trivial.

Induction step. Without loss of generality we can assume that f_1, f_2 are empty words. Consider a word x_iu of degree k, where $i = \overline{1,r}$. We have $\psi(T_2(x_iu,a)) = \psi(x_iux_iua) + \psi(ax_iux_iu) + \psi(x_iuax_iu) + \{(a),(b),(c)\}$. Induction hypothesis imply that $\psi(x_iux_iua) = \psi(u^2x_i^2a) + \{(a),(b),(c)\}$, $\psi(ax_iux_iu) = \psi(au^2x_i^2) + \{(a),(b),(c)\}$, $\psi(x_iuax_iu) = \psi(x_i^2u^2a) + \psi(x_i^2au^2) + \psi(u^2ax_i^2) + \psi(ax_i^2u^2) + \{(a),(b),(c)\}$. Thus, $\psi(T_2(x_iu,a)) = \psi(T_3(x_i^2,u^2,a)) + \{(a),(b),(c)\} = 0 + \{(a),(b),(c)\}$ by item 2. $\triangle$

Lemma 4 *Let $p = 3$. All identities of $N_{3,d}(1^d)$ are consequences of identities $f_1T_3(a_1,a_2,a_3)f_2$ of multidegree 1^d, where $f_1, f_2 \in F_d$, $a_1, a_2, a_3 \in F_d^{\#}$, $\deg(a_1) \leq 3$, $\deg(a_2) = \deg(a_3) = 1$.*

Proof. If $d \leq 4$, then the statement is obvious.

Let $d \geq 5$. We prove by induction on d.

Induction base. In the case $d = 5, 6$ the statement was proven by means of a computer programme.

Induction step. Let $d \geq 7$. Consider an identity $t = a_1 T_3(a_2, a_3, a_4) a_5$, $a_1, a_5 \in F_d$, $a_2, a_3, a_4 \in F_d^{\#}$. There is such $k = \overline{1,5}$ that $\deg(a_k) \geq 2$. Then $a_k = x_i x_j \cdot w$ for some $w \in F_d$. Substituting z for subword $x_i x_j$, where z is a new letter, and using induction hypothesis, we get that $t \in \mathrm{lin}\{f_1 T_3(b_1, b_2, b_3) f_2 |\ f_1, f_2 \in F_d,\ b_1, b_2, b_3 \in F_d^{\#},\ \deg(b_1 b_2 b_3) \leq 6\}$. The statement of the Lemma in the case $d = 6$ concludes the proof. $\triangle$

A multilinear word $w = x_{\sigma(1)} \cdots x_{\sigma(d)}$, $\sigma \in S_d$, is called *even*, if the permutation σ is even, and *odd* otherwise.

Lemma 5 1. *Let $p = 2, 3$. Consider the homomorphism $\phi : K\langle F_d\rangle(1^d) \to K$, defined by $\phi(w) = 1$, where $w \in F_d$. Then ϕ maps identities of $N_{3,d}$ in zero.*

2. *Let $p = 2$. For $i, j = \overline{1,d}$, $i \neq j$, consider the homomorphism $\phi_{ij} : K\langle F_d\rangle(1^d) \to K$, defined by the following way: if $w = u x_i x_j v$, where $u, v \in F_d$, then $\phi_{ij}(w) = 1$, else $\phi_{ij}(w) = 0$. Then ϕ_{ij} maps identities of $N_{3,d}$ in zero.*

3. *Let $p = 3$. Consider the homomorphism $\phi_+ : K\langle F_d\rangle(1^d) \to K$, defined by the following way: for $w \in F_d$ we have $\phi_+(w) = 1$, if w is even, else $\phi_+(w) = 0$. Then ϕ_+ maps identities of $N_{3,d}$ in zero.*

4. *Let $p = 3$. For $k = \overline{1,d}$ consider the homomorphism $\phi_k : K\langle F_d\rangle(\delta_1, \ldots, \delta_d) \to K\langle F_d\rangle(\delta_1, \ldots, \delta_{k-1}, \delta_{k+1}, \ldots, \delta_d)$, where $\delta_k = 1, 2$, defined by $\phi_k(x_{i_1} \cdots x_{i_t}) = y_{i_1} \cdots y_{i_t}$, where $y_{i_j} = x_{i_j}$, if $i_j \neq k$, and $y_{i_j} = 1$, if $i_j = k$ ($j = \overline{1,t}$, $t = \delta_1 + \cdots + \delta_d$). Then ϕ_k maps identities of $N_{3,d}$ in zero.*

5. *Let $p = 3$. For $k = \overline{1,d}$ consider the homomorphism $\pi_k : K\langle F_d\rangle(\delta_1, \ldots, \delta_{k-1}, 3, \delta_{k+1}, \ldots, \delta_d) \to K\langle F_d\rangle(\delta_1, \ldots, \delta_{k-1}, 1, \delta_{k+1}, \ldots, \delta_d)$, defined by the following way: for $w = u_1 x_k u_2 x_k u_3 x_k u_4$, $u_i \in F_d$ ($i = \overline{1,4}$), we put $\pi_k(w) = u_1(x_k u_2 u_3 + u_2 x_k u_3 + u_2 u_3 x_k) u_4$. Then π_k maps identities of $N_{3,d}$ in zero, and $\pi_i \pi_j (x_i^2 x_j^2 x_i x_j) = x_i x_j - x_j x_i$.*

Proof. 2. It is sufficient to proof that for $t = b_1 T_3(a_1, a_2, a_3) b_2$, where $b_1, b_2 \in F_d$, $a_1, a_2, a_3 \in F_d^{\#}$, we have $\phi_{ij}(t) = 0$. If each word from $\{b_1 a_{\sigma(1)} a_{\sigma(2)} a_{\sigma(3)} b_2 |\ \sigma \in S_3\}$ do not contain subword $x_i x_j$, then $\phi_{ij}(t) = 0$.

If there is k such that $a_k = u x_i x_j v$, $u, v \in F_d$, then $\phi_{ij}(t) = 6 = 0$.

If $b_1 = u x_i$, $a_1 = x_j v$, $u, v \in F_d$, then $\phi_{ij}(t) = 2 = 0$.

If $b_2 = x_j u$, $a_1 = v x_i$, $u, v \in F_d$, then $\phi_{ij}(t) = 2 = 0$.

If $a_1 = u x_i$, $a_2 = x_j v$, $u, v \in F_d$, then $\phi_{ij}(t) = 2 = 0$.

The statement follows from the regarded cases.

Items 3, 4, 5 were proved in [9]; item 1 is similar to them. $\triangle$

4 The case of $p \neq 3$, $d \leq 3$

Proposition 1 *Let $p \neq 3$, $d = \overline{1,3}$, $\Delta = (\delta_1, \ldots, \delta_d)$ is a multidegree. Then, the set B_Δ is a basis for $N_{3,d}(\Delta)$, where*

1) the case of $|\,\Delta| \leq 3$:

$B_1 = \{x_1\}$, $B_{1^2} = \{x_1x_2,\ x_2x_1\}$, $B_2 = \{x_1^2\}$,

$B_{1^3} = \{x_1x_2x_3,\ x_1x_3x_2,\ x_2x_1x_3,\ x_2x_3x_1,\ x_3x_1x_2\}$, $B_{21} = \{x_1^2x_2,\ x_2x_1^2\ \}$;

2) the case of $|\,\Delta| = 4$:

$B_{21^2} = \{x_1^2x_2x_3,\ x_1^2x_3x_2,\ x_2x_1^2x_3,\ x_2x_3x_1^2,\ x_3x_2x_1^2\}$,

$B_{2^2} = \{x_1^2x_2^2,\ x_2^2x_1^2\}$, $B_{31} = \{x_1^2x_2x_1\}$;

3) the case of $|\,\Delta| = 5$:

$B_{2^21} = \{x_1^2x_2^2x_3,\ x_2^2x_1^2x_3,\ x_3x_1^2x_2^2\}$,

$B_{31^2} = \{x_1^2x_2x_3x_1,\ x_1^2x_3x_2x_1\}$,

$B_{32} = \{x_1^2x_2^2x_1\}$;

4) otherwise $B_\Delta = \emptyset$.

Proof. Cases of $|\,\Delta| \leq 3$ and $\Delta \in \{31, 32\}$ follow from items $1, 2$ of Lemma 1.

If $\Delta \in \{21^2, 2^2, 2^21, 31^2\}$, then we prove the statement by considering the system of equations $\mathcal{S}_\Delta$. Here we use item 1 of Lemma 1; and when $\Delta \in \{21^2, 2^2, 2^21\}$, we use Lemma 3 for decreasing the number of considering equations.

Case 4) follows from item 3 of Lemma 1. $\triangle$

5 The case of $p = 0$ or $p > 3$

We shall write i for x_i, $i = \overline{1,d}$, so that it does not lead to ambiguity.

Proposition 2 *Let $p = 0$ or $p > 3$, $d \geq 1$, $\Delta = (\delta_1, \ldots, \delta_d)$ is a multidegree. Then the set B_Δ is a basis for $N_{3,d}(\Delta)$, where*

1) if $d \leq 3$, then see Proposition 1,

2) $B_{1^4} = \left\{ \begin{array}{lllll} 1234, & 1243, & 1324, & 1342, & 1423, \\ 2134, & 2143, & 2314, & 2341, & 2413, \\ 3124, & 3412 & & & \end{array} \right\}$,

3) $B_{1^5} = \left\{ \begin{array}{lllll} 12345, & 12354, & 12435, & 12453, & 12534, \\ 13245, & 13254, & 13425, & 13452, & 13524, \\ 14235, & 14523, & 23145, & 23415, & 23514 \end{array} \right\}$,

4) $B_{21^3} = \left\{ \begin{array}{llll} 1^2234, & 1^2324, & 1^2423, & \\ 21^234, & 21^243, & 231^24, & 241^23 \end{array} \right\}$,

5) if $|\,\Delta| \geq 6$, then $B_\Delta = \emptyset$.

Proof. The computations below were performed by means of a computer programme. For $\Delta \in \{1^4, 1^5, 21^4\}$, we consider the homogeneous system of linear equations $\mathcal{S}_\Delta$ over the ring, generated in $\mathcal{Q}$ by the set $\mathcal{Z} \cup \{1/2, 1/3\}$. Having expressed higher words in terms of lower words by the Gauss's method, we get that $\mathcal{S}_\Delta$ is equivalent to the system $\{1 \cdot u = f_u | \, u \in F_d, \, \mathrm{mdeg}(u) = \Delta, \, u \notin B_\Delta\}$, where f_u are linear combinations of elements of B_Δ. The statement is proven.

The case of $|\,\Delta| \geq 6$ follows from Lemma 1. $\triangle$

6 The composition method

Denote by M_5 a basis for the space of identities of $N_{3,5}(1^5)$ such that M_5 contains only reduced identities and all elements of M_5 have the highest terms pairwise different. The basis of this kind exists, because if t_1, t_2 are reduced identities with $\overline{t}_1 = \overline{t}_2$ and $t_1 \neq t_2$, then $\overline{t}_1 \neq \overline{t_1 - t_2}$ and $\mathrm{lin}\{t_1, t_2\} = \mathrm{lin}\{t_1, t_1 - t_2\}$. For $d \geq 5$, let

$$M_d = \{t \in K\langle F_d\rangle(1^d) |\text{ there are } t' \in M_5,\, \phi \in \mathcal{M}_{5,d},\, a \in F_d \text{ such that } t = a\phi(t')\}.$$

Identities from M_d are identities of $N_{3,d}$.

Let $\Delta = (\delta_1, \ldots, \delta_d)$ be a multidegree. For a set $J \subset K\langle F_d\rangle(\Delta)$, denote $B(J) = \{w \in F_d^{\#} | \, \mathrm{mdeg}(w) = \Delta, w \notin \overline{J}\}$. Since every word, of multidegree Δ, which do not belong to $B(J)$, can be expressed in terms of lower words by applying identities of J; therefore, for any $f \in K\langle F_d\rangle(\Delta)$, we have

$$f = \sum\nolimits_i \alpha_i t_i + \sum\nolimits_j \beta_j w_j, \text{ where } \alpha_i, \beta_j \in K,\, t_i \in J,\, w_j \in B(J),\, \overline{t_i}, w_j \leq \overline{f}. \quad (2)$$

Thus,

$$\frac{K\langle F_d\rangle(\Delta)}{\mathrm{lin}\, J} \simeq \mathrm{lin}\, B(J), \text{ and, in particular, } N_{3,d}(1^d) = \mathrm{lin}\, \Phi(B(M_d)), \quad (3)$$

where $\Phi : K\langle F_d\rangle^{\#} \to N_{3,d}$ is the natural homomorphism. Further, we will write $B(M_d)$ instead of $\Phi(B(M_d))$ so that it does not lead to ambiguity.

Definition. A set of reduced identities M is called *complete under composition*, if for any $t_1, t_2 \in M$, where $\overline{t}_1 = \overline{t}_2$, we have $t_1 - t_2 = \sum_{i=1}^{k} \alpha_i g_i$, $\alpha_i \in K$, $g_i \in M$, and $\overline{g}_i < \overline{t}_1$, $i = \overline{1,k}$.

Lemma 6 *For $d \geq 5$, all identities of $N_{3,d}(1^d)$ are consequences of identities of M_d.*

Proof. For any identity t of $N_{3,d}(1^d)$, we have $t = \sum_i \alpha_i t_i$ for some $\alpha_i \in K$, $t_i = f_i T_3(a_i, b_i, c_i) g_i$, $f_i, g_i \in F_d$, $a_i, b_i, c_i \in F_d^{\#}$. For any i, exists $\phi_i \in \mathcal{M}_{5,d}$ and an identity t'_i, of $N_{3,5}(1^5)$, such that $t_i = \phi_i(t'_i)$. The set M_5 is a basis for the space of identities of $N_{3,5}(1^5)$, thus $t'_i = \sum_j \beta_{ij} g_{ij}$, where $g_{ij} \in M_5$, $\beta_{ij} \in K$. Hence $\phi_i(t'_i) = \sum_j \beta_{ij}\phi_i(g_{ij}) \in \operatorname{lin} M_d$. Therefore, $t \in \operatorname{lin} M_d$. $\triangle$

Lemma 7 *(Composition Lemma [2]) For $d \geq 5$ $B(M_d)$ is a basis for $N_{3,d}(1^d)$ if and only if M_d is complete under composition.*

Proof. Let $B(M_d)$ be a basis for $N_{3,d}(1^d)$. For $t_1, t_2 \in M_d$, where $\overline{t}_1 = \overline{t}_2$, let $g = t_1 - t_2$. By formula (2) we have $g = \sum_i \alpha_i f_i + \sum_j \beta_j w_j$, where $\overline{f}_i \leq \overline{g} < \overline{t}_1$, $f_i \in M_d$, $w_i \in B(M_d)$, $\alpha_i, \beta_j \in K$. The identity $g - \sum_i \alpha_i f_i$ is an identity of $N_{3,d}$, $B(M_d)$ is a basis for $N_{3,d}(1^d)$, hence $\sum_j \beta_j w_j = 0$ in $K\langle F_d\rangle$. Thus $g = \sum_i \alpha_i f_i$, and the claim is proven.

Let M_d be complete under composition. Assume that, on the contrary, $B(M_d)$ is not a basis. Thus, the set $B(M_d)$ is linearly dependent in $N_{3,d}$ (see equality (3)). Hence there is a non-trivial identity $f = \sum_i \alpha_i u_i$, $\alpha_i \in K$, $u_i \in B(M_d)$, such that $f = 0$ in $N_{3,d}$. Note that $\overline{f} \notin \overline{M}_d$.

Lemma 6 implies $f = \sum_{j=1}^{k} \beta_j t_j$, where $\beta_j \in K^*$, $t_j \in M_d$. Without loss of generality, we can assume that for some s, we have $\overline{t}_1 = \cdots = \overline{t}_s = \overline{f}$. If $s = 1$ then we get a contradiction to $\overline{f} \notin \overline{M}_d$. Let $s \geq 2$. Since M_d is complete under composition, for $j = \overline{2, s}$ we have $t_1 - t_j = \sum_l \gamma_{jl} g_{jl}$, where $g_{jl} \in M_d$, $\overline{g}_{jl} < \overline{t}_1$, $\gamma_{jl} \in K$. Expressing t_j from these equalities, we get $f = \lambda t_1 + \sum_q \lambda_q h_q$ for some $h_q \in M_d$, $\overline{h}_q < \overline{t}_1$, $\lambda, \lambda_q \in K$. If $\lambda \neq 0$, then $\overline{f} \in \overline{M}_d$, so we get a contradiction. Thus, $\lambda = 0$. Repeating the same argument several times, we get a contradiction to the non-triviality of f. $\triangle$

Lemma 8 *Let $d \geq 5$. Then for any $t_1, t_2 \in M_d$, where $\overline{t}_1 = \overline{t}_2$, there are $s = \overline{5, 10}$, $t'_1, t'_2 \in M_s$, $\phi \in \mathcal{M}_{s,d}$, $a \in F_d$ such that $t_i = a\phi(t'_i)$, where $i = 1, 2$.*

Proof. By definition of M_d, there are $t''_i \in M_5$, $\psi_i \in \mathcal{M}_{5,d}$, $c_i \in F_d$ such that $t_i = c_i \psi_i(t''_i)$, where $i = 1, 2$. Denote $w = \overline{t}_1 = \overline{t}_2$. Let $\overline{t}''_1 = x_{j_1} \cdots x_{j_5}$, $\overline{t}''_2 = x_{k_1} \cdots x_{k_5}$. Consider a partition of w into subwords $w = a \cdot a_1 \cdot \cdots \cdot a_s$, where $s = \overline{5, 10}$, $a_1, \ldots, a_s \in F_d^{\#}$, $a \in F_d$, which is the result of intersection of partitions $w = \overline{t}_1 = c_1 \cdot \psi_1(x_{j_1}) \cdot \cdots \cdot \psi_1(x_{j_5})$, $w = \overline{t}_2 = c_2 \cdot \psi_2(x_{k_1}) \cdot \cdots \cdot \psi_2(x_{k_5})$. Here we assume $a \neq 1$ if and only if c_1, c_2 are non-empty words. Then $c_i = a d_i$, where $d_i \in F_d$, $i = 1, 2$. There is a permutation $\sigma \in S_s$ such that if $x_i < x_j$, then $a_{\sigma(i)} < a_{\sigma(j)}$, where $i, j = \overline{1, s}$. Since $d_1\psi_1(t''_1), d_2\psi_2(t''_2)$ are elements generated by words $a_1, \ldots, a_s$, the substitutions $d_i\psi_i(t''_i)|_{a_{\sigma(j)} \to x_j, j=\overline{1,s}} = t'_i$, $i = 1, 2$, are well-defined. It is easy to see

that for t'_i there is $\psi'_i \in \mathcal{M}_{5,s}$, $e_i \in F_s$ such that $e_i\psi'_i(t''_i) = t'_i$, i.e. $t'_i \in M_s$, where $i = 1, 2$. Define $\phi \in \mathcal{M}_{s,d}$ by the following way: $\phi(x_j) = a_{\sigma(j)}$, $j = \overline{1, s}$. We have $a\phi(t'_i) = t_i$, where $i = 1, 2$, thus the claim is proven. $\triangle$

Proposition 3 *If $B(M_d)$ is a basis for $N_{3,d}(1^d)$ for $d = \overline{5, 10}$, then $B(M_d)$ is a basis for $N_{3,d}(1^d)$ for any $d \geq 5$.*

Proof. Let $d \geq 11$. Consider $t_1, t_2 \in M_d$, where $\overline{t}_1 = \overline{t}_2$. We apply Lemma 8 to t_1, t_2; further we use the notation from Lemma 8. By the data and Lemma 7 M_s is complete under composition, hence $t'_1 - t'_2 = \sum_i \alpha_i g'_i$, where $\alpha_i \in K$, $g'_i \in M_s$, $\overline{t}'_1 > \overline{g}'_i$. Thus $t_1 - t_2 = \sum_i \alpha_i g_i$, where $g_i = a\phi(g'_i) \in M_d$; because of the composition of monotonous substitutional mappings is a monotonous substitutional mapping. By monotony of ϕ, we have $\overline{t}_1 > \overline{g}_i$ for all i. Hence M_d is complete under composition, and Lemma 7 concludes the proof. $\triangle$

7 Multilinear homogeneous component

Notation. For $p = 2, 3$ and $d \geq 1$ recursively define sets B_{1^d} of the words of multidegree 1^d.

Let $p = 2$. Then

1) $B'_1 = \{x_1\}$;

2) for $d \geq 2$ define $B'_{1^d} = x_1\{B_{1^{d-1}}|_{x_i \to x_{i+1},\, i=\overline{1,d-1}}\} \cup \{\underline{e}_{d,k} |\, k = \overline{2, d}\} \cup \{\underline{f}_d\} \cup \{\underline{h}_{d,k} |\, k = \overline{3, d}\}$.

Here, if $i \geq 1, i \neq 4$, then $B_{1^i} = B'_{1^i}$; $B_{1^4} = B'_{1^4} \cup \{x_2x_1x_4x_3\}$ and

$\underline{e}_{d,k} = x_2 \cdots x_k \cdot x_1 \cdot x_{k+1} \cdots x_d$ $(d \geq 2,\ k = \overline{2, d})$;

$\underline{f}_d = x_2 \cdots x_{d-2} \cdot x_d x_1 x_{d-1}$ $(d \geq 3)$;

$\underline{h}_{d,k} = x_k \cdot x_1 \cdots \widetilde{x}_k \cdots x_d$ $(d \geq 3,\ k = \overline{3, d})$.

Let $p = 3$. Then

1) $B_1 = \{x_1\}$;

2) for $d \geq 2$ define $B_{1^d} = x_1\{B_{1^{d-1}}|_{x_i \to x_{i+1},\, i=\overline{1,d-1}}\} \cup x_2\{B_{1^{d-1}}|_{x_i \to x_{i+1},\, i=\overline{2,d-1}}\} \cup \{\underline{e}_{d,k} |\, k = \overline{3, d}\}$.

Here, $\underline{e}_{d,k} = x_3 \cdots x_k \cdot x_1x_2 \cdot x_{k+1} \cdots x_d$ $(d \geq 3,\ k = \overline{3, d})$.

For future needs define $B_{1^0} = \{1\}$, where 1 stands for the empty word.

The aim of this section is to prove the following theorem:

Theorem 1 *For $p = 2, 3$, $d \geq 1$ the set B_{1^d} is a basis for $N_{3,d}(1^d)$.*

Remark 2 *It is not difficult to see that*

$$|B_{1^d}| = \left\{ \begin{array}{lcc} d(d-1) & , & p=2,\, d\geq 4 \\ 2^d - d & , & p=3 \end{array} \right. .$$

Let V be a finite dimensional vector space over K, $V = \mathrm{lin}\{v_1, \ldots, v_m\}$, where non-zero vectors $\{v_i\}$ are linearly ordered by the following way: $v_1 < \cdots < v_m$. Note that the vectors $v_1, \ldots, v_m$ need not be linearly independent.

Definition. A basis of V $v_{k_1}, \ldots, v_{k_s}$ is called *minimal* (with respect to the linearly ordered set $v_1, \ldots, v_m$), if for any $i = \overline{1, m}$ we have $v_i = \sum_j \alpha_{ij} v_{k_j}$, $\alpha_{ij} \in K$, where $k_j \leq i$.

Consider $L_1 = \{v_{j_1}, \ldots, v_{j_s}\}$, $L_2 = \{v_{k_1}, \ldots, v_{k_s}\}$ which are bases for V, where $j_1 < \cdots < j_s$, $k_1 < \cdots < k_s$. We write $L_1 < L_2$, if there is $l = \overline{1, s}$ such that $j_1 = k_1, \ldots, j_{l-1} = k_{l-1}, j_l < k_l$.

Lemma 9 1. *A basis of V $v_{k_1}, \ldots, v_{k_s}$ is minimal (with respect to the linearly ordered set $v_1, \ldots, v_m$) if and only if it is the least one with respect to the determined linear order.*

2. *The minimal basis is uniquely determined.*

Proof. 1. Let L be the minimal basis. Then

$$\text{if } v_k \notin \mathrm{lin}\{v_1, \ldots, v_{k-1}\}, \text{ then } v_k \in L; \text{ else } v_k \notin L \ (k = \overline{1, m}). \tag{4}$$

Thus, L is the least basis.

Let $L \subset \{v_1, \ldots, v_m\}$ be the least basis. Then condition (4) is valid for it. Thus L is the minimal basis.

2. This item follows from item 1. $\triangle$

Apply aforesaid on minimal bases to $N_{3,d}(1^d)$. As a linearly ordered set we take $\{w \in F_d |\ \mathrm{mdeg}(w) = 1^d\}$.

Lemma 10 1. *$B(M_5)$ is a basis for $N_{3,d}(1^5)$.*

2. *Let $d \geq 5$. If $B(M_d)$ is a basis for $N_{3,d}(1^d)$, then $B(M_d)$ is the minimal basis.*

Proof. 1. The definition of M_5 implies that M_5 is complete under composition. Lemma 7 concludes the proof.

2. Identities M_d imply that any word, of $N_{3,d}$, which do not belong to $B(M_d)$ can be expressed in terms of lower words. Thus $B(M_d)$ is the minimal basis. $\triangle$

Lemma 11 1. *If $p = 2$, then for $i = 4, 5$ the minimal basis for $N_{3,i}(1^i)$ is B_{1^i}, and*

$$B_{1^4} = \left\{ \begin{array}{lllll} 1234, & 1243, & 1324, & 1342, & 1423, \\ 2134, & 2143, & 2314, & 2341, & 2413, \\ 3124, & 4123 & & & \end{array} \right\};$$

$$B_{1^5} = B(M_5) = \left\{ \begin{array}{lllll} 12345, & 12354, & 12435, & 12453, & 12534, \\ 13245, & 13254, & 13425, & 13452, & 13524, \\ 14235, & 15234, & & & \\ 21345, & 23145, & 23415, & 23451, & \\ 23514, & & & & \\ 31245, & 41235, & 51234 & & \end{array} \right\}.$$

2. *If $p = 3$, then for $i = 4, 5$ the minimal basis for $N_{3,i}(1^i)$ is B_{1^i}, and*

$$B_{1^4} = \left\{ \begin{array}{lllll} 1234, & 1243, & 1324, & 1342, & 1423, \\ 2134, & 2143, & 2314, & 2341, & 2413, \\ 3124, & 3412 & & & \end{array} \right\};$$

$$B_{1^5} = B(M_5) = \left\{ \begin{array}{lllll} 12345, & 12354, & 12435, & 12453, & 12534, \\ 13245, & 13254, & 13425, & 13452, & 13524, \\ 14235, & 14523, & & & \\ 21345, & 21354, & 21435, & 21453, & 21534, \\ 23145, & 23154, & 23415, & 23451, & 23514, \\ 24135, & 24513, & & & \\ 31245, & 34125, & 34512 & & \end{array} \right\}.$$

Proof. By Lemma 10, $B(M_5)$ is the minimal basis for $N_{3,5}(1^5)$, and, in particular, it does not depend on the choice of M_5 (see Lemma 9). Expressing higher words in terms of lower words by Gauss's method, we solve the system $\mathcal{S}_{1^d}$ and find the minimal basis for $N_{3,d}(1^d)$. These calculations were performed by means of a computer programme for $d = 4, 5$, $p = 2, 3$. $\triangle$

Lemma 12 *If $p = 2$, $d \geq 5$, then*

$$\overline{M}_d = \left\{ \begin{array}{ll} w_3 = ua_1a_2a_3, & a_1 > a_2 > a_3, \\ w_{4,1} = ua_1a_2a_3a_4, & a_1 > a_2, a_4 \text{ and } a_3 > a_4, \\ w_{4,2} = ua_1a_2a_3a_4, & a_1 > a_4 \text{ and } a_2 > a_3, \\ w_{5,1} = ua_1a_2a_3a_4a_5, & a_1 > a_2 \quad \text{and} \quad a_3 > a_4 \text{ or } a_3 > a_5 \text{ or } a_4 > a_5, \\ w_{5,2} = ua_1a_2a_3a_4a_5, & a_1 > a_3 \quad \text{and} \quad a_2 > a_4 \text{ or } a_2 > a_5 \text{ or } a_4 > a_5, \\ w_{5,3} = ua_1a_2a_3a_4a_5, & a_1 > a_4 \text{ and } a_2 > a_5. \end{array} \right\},$$

where all elements of $\overline{M}_d$ are words of multidegree 1^d, $u \in F_d$, $a_i \in F_d^{\#}$, $i = \overline{1,5}$.

If $p = 3$, $d \geq 5$, then

$$\overline{M}_d = \left\{ \begin{array}{ll} w_3 = ua_1a_2a_3, & a_1 > a_2 > a_3, \\ w_4 = ua_1a_2a_3a_4, & a_1 > a_2, a_4, \\ w_{5,1} = ua_1a_2a_3a_4a_5, & a_1 > a_2, a_3 \ and \ a_4 > a_5, \\ w_{5,2} = ua_1a_2a_3a_4a_5, & a_1 > a_3, a_4 \ and \ a_2 > a_5, \\ w_{5,3} = ua_1a_2a_3a_4a_5, & a_1 > a_4, a_5 \ and \ a_2 > a_3. \end{array} \right\},$$

where all elements of $\overline{M}_d$ are words of multidegree 1^d, $u \in F_d$, $a_i \in F_d^{\#}$, $i = \overline{1,5}$.

Proof. It is sufficient to prove the statement for $d = 5$. Denote by M the set from the formulation of the Lemma. Considering all possibilities, we get that $B(M_5) = \{w \in F_5 |\ \mathrm{mdeg}(w) = 1^5,\ w \notin M\}$ (see Lemma 11). $\triangle$

Lemma 13 *For $p = 2, 3$, $d \geq 5$ we have $B(M_d) = B_{1^d}$.*

Proof. For $p = 2, 3$ we get $B_{1^d} \subset B(M_d)$ by Lemma 12.

Further $w_{i,j}, w_i$ stand for the words from Lemma 12.

The case of p = 2. Inclusion $B(M_d) \subset B_{1^d}$ follows from items 1, 2 (see below) by induction on d.

1. *If $w = x_{i_1} \cdots x_{i_d} \in B(M_d)$, $i_1 \geq 3$, then $w = \underline{h}_{d,i_1}$.*

Proof. Let $w = x_{i_1}u$. The word w contains letters x_1, x_2. Denote by u_1, u_2, u_3 some elements of F_d. If $u = u_1x_2u_2x_1u_3$, then $w = w_3 \in \overline{M}_d$, that is a contradiction. Hence $u = u_1x_1u_2x_2u_3$. If the word u_1 is not empty, then $w = w_{4,2} \in \overline{M}_d$, that is a contradiction. If the word u_2 is not empty, then $w = w_{4,1} \in \overline{M}_d$, that is a contradiction. Assume that $u_3 = x_{j_1} \cdots x_{j_s}$ and there are k, t such that $k < t \leq s$ and $j_k > j_t$. Then $w = w_{5,1} \in \overline{M}_d$, that is a contradiction. Hence $w = \underline{h}_{d,i_1}$.

2. *If $w = x_2x_{i_2} \cdots x_{i_d} \in B(M_d)$, then $w = \underline{e}_{d,k}$ for some $k = \overline{2,d}$ or $w = \underline{f}_d$.*

Proof. Consider $w = x_2u_1x_1u_2$, where $u_1, u_2 \in F_d$. If there are not r, s such that $r > s$ and $u_1u_2 = v_1x_rv_2x_sv_3$, where $v_1, v_2, v_3 \in F_d$, then $w = \underline{e}_{d,k}$ for some $k = \overline{2,d}$. Assume that there are such r, s. If the word v_3 contains the letter x_1, then $w = w_{4,2} \in \overline{M}_d$; a contradiction. If the word v_1 contains the letter x_1, then $w = w_{5,1}$ or $w = w_{5,2}$, hence $w \in \overline{M}_d$; a contradiction. Let the word v_2 contains the letter x_1. If the word v_3 is not empty, then $w = w_{5,2} \in \overline{M}_d$; a contradiction. If $\deg(v_2) > 1$, then $w = w_{5,2}$ or $w = w_{5,3}$, hence $w \in \overline{M}_d$; a contradiction. There is the only possibility which we have not considered, namely $w = \underline{f}_d$.

The case of p = 3. Inclusion $B(M_d) \subset B_{1^d}$ follows from items 1, 2 (see below) by induction on d.

1. *If $w = x_{i_1} \cdots x_{i_d}$, $i_1 \geq 4$, then $w \notin B(M_d)$.*

Proof. The word $w_1 = x_{i_2} \cdots x_{i_d}$ contains the letters x_1, x_2, x_3. There are $r, s = \overline{1,3}$ such that the word w_1 contains some letters between letters x_r, x_s. We also have $x_{i_1} > x_r, x_s$. Thus $w = w_4 \in \overline{M}_d$, that is $w \notin B(M_d)$.

2. *If $w = x_3 x_{i_2} \cdots x_{i_d} \in B(M_d)$, then $w = \underline{e}_{d,k}$ for some $k = \overline{3,d}$.*

Proof. If $w = x_3 u_1 x_2 u_2 x_1 u_3$ for some elements u_1, u_2, u_3 of F_d, then $w = w_3 \in \overline{M}_d$; a contradiction. Thus $w = x_3 u_1 x_1 u_2 x_2 u_3$. If the word u_2 is not empty, then $w = w_4 \in \overline{M}_d$, that is a contradiction. Hence $u = x_3 u_1 x_1 x_2 u_3$. If there are r, s such that $r > s$ and $u_1 u_3 = v_1 x_r v_2 x_s v_3$ for some $v_1, v_2, v_3 \in F_d$, then $w = w_{5,1}$ or $w = w_{5,2}$ or $w = w_{5,3}$. Therefore $w \in \overline{M}_d$, that is a contradiction. Hence there are not such r, s. So $w = \underline{e}_{d,k}$ for some $k = \overline{3,d}$. $\triangle$

Lemma 14 *Let $p = 3$, $d \geq 6$, ϕ_k is the mapping from Lemma 5, where $k = \overline{1,d}$. Then for any $w \in B(M_d)$ we have $\phi_k(w)|_{x_i \to x_{i-1}, i=\overline{k+1,d}} \in B(M_{d-1})$.*

Proof. If for a word w of multidegree 1^d we have $\phi_k(w)|_{x_i \to x_{i-1}, i=\overline{k,d}} \in \overline{M}_{d-1}$, then $w \in \overline{M}_d$, that is $w \notin B(M_d)$. $\triangle$

Proof of theorem 1. If $d = 1, 2, 3$ then obviously B_{1^d} is a basis. For $d = 4, 5$ B_{1^d} is a basis by Lemma 11. Proposition 3 and Lemma 13 imply that in order to prove the Theorem it is sufficient to verify that B_{1^d} is linearly independent in $N_{3,d}$ for $d = \overline{6, 10}$. This verification was done by means of a computer programme applying the algorithm described below.

The case of $\mathbf{p = 2}$. Assume that there is an identity $f = \sum_{w \in B_{1^d}} \alpha_w w$, $\alpha_w \in K$, such that $f = 0$ in $N_{3,d}$. Considering $\phi_{ij}(t) = 0$, $\phi(t) = 0$, where ϕ_{ij}, ϕ are mappings from Lemma 5, we get a homogeneous system of linear equations in $\{a_w\}$. Having solved this system we get that $\alpha_w = 0$ for any $w \in B_{1^d}$. It was calculated for $d = \overline{6, 10}$ by means of a computer programme.

The case of $\mathbf{p = 3}$. By Lemma 13, we have $B_{1^d} = B(M_d)$. Identities from M_5 express elements of the set $\{w \in F_5 |\, \mathrm{mdeg}(w) = 1^5\}$ in terms of elements of B_{1^5}. Applying these identities, we get that for any word w of multidegree 1^d $w = f_w$ in $N_{3,d}$, where $f_w \in \mathrm{lin}\, B_{1^d}$. Applying identities $\{w = f_w\}$, rewrite identities $\{f_1 T_3(a_1, a_2, a_3) f_2 |\, f_1, f_2 \in F_d, \deg(a_1) \leq 3, \deg(a_2) = \deg(a_3) = 1\}$ in terms of linear combinations of the elements of B_{1^d}. As a result, we get only trivial identities. This, together with Lemma 4, imply that the system of identities $\mathcal{S}_{1^d}$ is equivalent to the set of identities $M = \{w - f_w |\, w \in F_d, \mathrm{mdeg}(w) = 1^d,\, w \notin B_{1^d}\}$. The set M is linearly independent in $K\langle F_d \rangle$, thus B_{1^d} is linearly independent in $N_{3,d}$. The given algorithm performed by means of a computer programme proved that B_{1^d} is linearly independent in $N_{3,d}$ when $d = \overline{6, 9}$. Here we need Lemma 4 in order to decrease the quantity of identities which have to be considered. For $d = 10$ described algorithm ran for a long time, thus we used another approach to the case of $d = 10$.

Assume that there is an identity $f = \sum_{w \in B_{1^d}} \alpha_w w$, where $\alpha_w \in K$, such that $f = 0$ in $N_{3,d}$. Consider mappings ϕ_k ($k = \overline{1,d}$), ϕ_+ from Lemma 5. We assume

that $B_{1^{d-1}}$ is linearly independent in $N_{3,d}$. Hence, we get a homogeneous system of linear equations in $\{\alpha_w\}$ (see also Lemma 14). For even $d=\overline{6,10}$ it was calculated by means of a computer programme that this system has the only solution $\alpha_w=0$ for any $w\in B_{1^d}$. $\triangle$

8 The case of $p=2$

Let $d\geq 4$, $i,j=\overline{2,d}$, $i\neq j$. Introduce notations for some words of multidegree 21^{d-1}: $\underline{a}_i=x_1^2x_ix_2\cdots\widetilde{x}_i\cdots x_d$, $\underline{b}_i=x_1\cdots\widetilde{x}_i\cdots x_dx_ix_1^2$, $\underline{c}_{ij}=x_ix_1^2x_jx_2\cdots\widetilde{x}_i\cdots\widetilde{x}_j\cdots x_d$, if $i<j$, and $\underline{c}_{ij}=x_ix_1^2x_jx_2\cdots\widetilde{x}_j\cdots\widetilde{x}_i\cdots x_d$, if $i>j$. By items 1, 7 of Lemma 1 we have

$$N_{3,d}(21^{d-1})=\mathrm{lin}\{\underline{a}_i,\underline{b}_i,\underline{c}_{ij}\,|\,i,j=\overline{2,d},\ i\neq j\}. \qquad (5)$$

Theorem 2 *Let $p=2$, $d\geq 1$.*

1. For $\Delta=(\delta_1,\ldots,\delta_d)$, $d\leq 3$ a basis for $N_{3,d}(\Delta)$ is the set B_Δ defined in Proposition 1.

2. For $d\geq 4$ a basis for $N_{3,d}(1^d)$ is the set B_{1^d} defined above.

3. A basis for $N_{3,4}(21^3)$ is the set $B_{21^3}=\{\underline{a}_i,\underline{b}_i,\underline{c}_{23},\underline{c}_{32}\,|\,i=\overline{2,4}\}$.
For $d\geq 5$ a basis for $N_{3,d}(21^{d-1})$ is the set $B_{21^{d-1}}=\{\underline{a}_i,\underline{b}_i,\underline{c}_{23}\,|\,i=\overline{2,d}\}$.

4. For $d\geq 4$ a basis for $N_{3,d}(2^21^{d-2})$ is the set $B_{2^21^{d-2}}=\{x_1^2x_2^2x_3\cdots x_d,x_2^2x_1^2x_3\cdots x_d\}$.

5. For $d\geq 4$ a basis for $N_{3,d}(31^{d-1})$ is the set $B_{31^{d-1}}=\{x_1^2x_2\cdots x_dx_1\}$.

6. The rest of $\mathcal{N}^d$-homogeneous components of $N_{3,d}$ are equal to zero.

In order to prove item 3 we need the following Lemma.

Denote $h_{ij}=\underline{b}_i+\underline{c}_{ij}+\underline{a}_j$. Consider identities of multidegree 21^{d-1}:

$$\begin{array}{rcl}
M_0 &=& \{f_1I_i(x_1,a,b,c)f_2\,|\,i=\overline{1,3}\},\\
M_1 &=& \text{the set of identities (a) from Lemma 2},\\
M_2 &=& \{f_1T_3(x_1^2,a,b)f_2\},\\
M_3 &=& \{T_3(x_1^2,x_i,x_j)a,\ aT_3(x_1^2,x_i,x_j)\,|\,2\leq i<j\leq d\},\\
M_4 &=& \left\{\begin{array}{l}\{h_{23}+h_{34},h_{23}+h_{42},h_{32}+h_{24},h_{32}+h_{43}\},\text{if } d=4\\ \{h_{23}+h_{ij}\,|\,2\leq i\neq j\leq d,\ i\neq 2\text{ or } j\neq 3\},\text{if } d\geq 5,\end{array}\right.
\end{array}$$

where $a,b,c\in F_d^{\#}$, $f_1,f_2\in F_d$. For $i=\overline{1,4}$ denote $L_i=\mathrm{lin}\{M_0\cup M_i\}$.

Lemma 15 *Let $p=2$, $d\geq 4$. Then*

1. $L_1=L_2$.

2. $L_2 = L_3$.

3. $L_3 = L_4$.

Proof. Let $i, j, k, l \in \overline{2, d}$ be pairwise different numbers.

1. Inclusion $L_2 \subset L_1$ is obvious.

Consider an identity $t \in M_1$.

If $t = T_3(ax_1^2 b, c, d)$, then $t = aI_1(x_1, b, c, d) + I_2(x_1, c, d, a)b + I_3(x_1, ca, b, d) + dI_3(x_1, a, b, c) + 2dcax_1^2 b$.

If $t = T_3(x_1^2 a, b, c)$, then $t = I_1(x_1, a, b, c) + I_3(x_1, c, a, b) + I_3(x_1, b, a, c)$.

If $t = x_1^2 a T_3(b, c, d)$, then $t = I_1(x_1, a, b, c)d + I_1(x_1, a, b, d)c + I_1(x_1, a, c, d)b$.

If $t = x_1^2 T_3(a, b, c)$, then $t = I_1(x_1, a, b, c) + I_1(x_1, b, a, c) + I_1(x_1, c, a, b)$.

Thus we get $L_1 \subset L_2$.

3. Introduce notations for identities:

$$f_{ijk} = \underline{a}_i + \underline{a}_j + \underline{c}_{ij} + \underline{c}_{ji} + \underline{c}_{ik} + \underline{c}_{jk} = T_3(x_1^2, x_i, x_j)x_k a + \{M_0\},$$
$$g_{ijk} = \underline{b}_j + \underline{b}_k + \underline{c}_{jk} + \underline{c}_{kj} + \underline{c}_{ij} + \underline{c}_{ik} = ax_i T_3(x_1^2, x_j, x_k) + \{M_0\},$$

where $a \in F_d$. We have

$$f_{ijk} + g_{jik} = h_{ki} + h_{ij} \in L_3. \tag{6}$$

If $d = 4$, then formula (6) implies $L_4 \subset L_3$.

If $d \geq 5$, then replacing indices in formula (6) we get $h_{ij} + h_{jk} \in L_3$, $h_{ij} + h_{jl} \in L_3$, $h_{jl} + h_{lk} \in L_3$, $h_{lk} + h_{kj} \in L_3$. Add up last four formulas and get $h_{jk} + h_{kj} \in L_3$. Thus $h_{ij} + h_{ji}, h_{ij} + h_{jk} \in L_3$. Therefore $L_4 \subset L_3$.

From $f_{ijk} = 4h_{23} + h_{ij} + h_{ji} + h_{ik} + h_{jk} \in L_4$, $g_{ijk} = 4h_{23} + h_{jk} + h_{kj} + h_{ik} + h_{ij} \in L_4$ we can see that $L_3 \subset L_4$ for $d \geq 5$.

Let $d = 4$. Equalities $f_{ijk} = f_{jik}$, $g_{ijk} = g_{ikj}$, $f_{234} + f_{243} = f_{342}$, $g_{234} + g_{324} = g_{423}$,

$$\begin{aligned}
f_{234} &= (h_{23} + h_{34}) + (h_{32} + h_{24}), \\
f_{243} &= (h_{23} + h_{42}) + (h_{32} + h_{24}) + (h_{32} + h_{43}), \\
g_{234} &= (h_{23} + h_{34}) + (h_{32} + h_{24}) + (h_{32} + h_{43}), \\
g_{324} &= (h_{23} + h_{34}) + (h_{23} + h_{42}) + (h_{32} + h_{24}),
\end{aligned}$$

imply $L_3 \subset L_4$.

2. Inclusion $L_3 \subset L_2$ is obvious.

Consider an identity $t \in M_2$.

If $t = T_3(x_1^2, a, bc)$, then $t = T_3(x_1^2, a, b)c + bT_3(x_1^2, a, c) + \{M_0\}$.

If $d \geq 5$, then for $t = f_1 x_k T_3(x_1^2, x_i, x_j)x_l f_2$, $f_1, f_2 \in F_d$, we have $t = \underline{c}_{ki} + \underline{c}_{kj} + \underline{c}_{ij} + \underline{c}_{ji} + \underline{c}_{il} + \underline{c}_{jl} + \{M_0\} \in L_4$; thus $t \in L_3$ by item 3.

Therefore $L_2 \subset L_3$. $\triangle$

Proof of theorem 2. 2. See Theorem 1.

3. By equality (5) and identities M_4 it is sufficient to show that $B_{21^{d-1}}$ is linear independent in $N_{3,d}$.

Lemmas 2 and 15 imply that all identities, of $N_{3,d}(21^{d-1})$, generated by $x_1^2, x_2, \ldots, x_d$ are consequences of identities $M_0 \cup M_4$. Let f be a mapping such that the image of a word w, generated by $x_1^2, x_2, \ldots, x_d$, of multidegree 21^{d-1} is equal to the result of application of the identities from item 7 of Lemma 1 to w, i.e. $f(w)$ is equal to $\underline{a}_i$, $\underline{b}_i$ or $\underline{c}_{ij}$ for some i, j. Identities $M_0 \cup M_4$ are equivalent to the identities $M_0' \cup M_4 = M$, where $M_0' = \{w + f(w) | w$ is a word, $\mathrm{mdeg}(w) = 21^{d-1}$, $w \neq f(w)\}$. Every identity of M_0' (M_4, respectively) contains a word which is not a summand of any element of $B_{21^{d-1}}$ and is a summand of one and only one identity of M (M_4, respectively). Moreover we can assume that regarded words are pairwise different. Thus item 2 of Remark 1 implies that $B_{21^{d-1}}$ is linearly independent in $N_{3,d}$.

4. Denote $a = x_1^2 x_2^2 x_3 \cdots x_d$, $b = x_2^2 x_1^2 x_3 \cdots x_d$. By items 1, 4 and 7 of Lemma 1, we have $\mathrm{lin}\{a, b\} = N_{3,d}(2^2 1^{d-2})$. We claim that a, b are linearly independent in $N_{3,d}$. Consider the homomorphism of vector spaces $\psi : K\langle F_d \rangle \to K\langle F_d \rangle (2^2 1^{d-2})$ defined by the following way: for a word w $\psi(w) = \alpha a + \beta b$, where α (β, respectively) is equal to the number of subwords $x_1 x_2$ ($x_2 x_1$, respectively) in the word w.

For $u, v \in F_d^{\#}$ define

$$\psi(u, v) = \begin{cases} a & , \text{ if } u = u_1 x_1,\ v = x_2 v_1\ (u_1, v_1 \in F_d) \\ b & , \text{ if } u = u_1 x_2,\ v = x_1 v_1\ (u_1, v_1 \in F_d) \\ 0 & , \text{ otherwise} \end{cases} .$$

It is easy to see that for $u_1, \ldots, u_s \in F_d^{\#}$

$$\psi(u_1 \cdots u_s) = \sum_{i=1}^{s} \psi(u_i) + \sum_{i=1}^{s-1} \psi(u_i, u_{i+1}). \tag{7}$$

Consider an identity t of $\mathcal{S}_{2^2 1^{d-2}}$.

If $t = f_1 T_1(g) f_2$, $f_1, f_2 \in F_d$, $g \in F_d^{\#}$, then $t \notin \mathcal{S}_{2^2 1^{d-2}}$. It is a contradiction.

If $t = f_1 T_2(g_1, g_2) f_2$, $f_1, f_2 \in F_d$, $g_1, g_2 \in F_d^{\#}$, then $\psi(t) = \psi(g_2) + \psi(f_1) + \psi(f_2) + \psi(f_1, g_2) + \psi(g_2, f_2)$, by equality (7). The multidegree of t is $2^2 1^{d-2}$, thus $g_1 \in \{x_1, x_2, x_1 x_2, x_2 x_1\}$. Hence $\psi(t) = 0$.

If $t = f_1 T_3(g_1, g_2, g_3) f_2$, $f_1, f_2 \in F_d$, $g_1, g_2, g_3 \in F_d^{\#}$, then $\psi(t) = 0$ by equality (7).

Therefore $\psi(t) = 0$ for any identity t of $N_{3,d}(2^2 1^{d-2})$.

If $t = \alpha a + \beta b$, $\alpha, \beta \in K$, is an identity of $N_{3,d}$, then $\psi(t) = \alpha a + \beta b = 0$ in $K\langle F_d \rangle$. Hence $\alpha = \beta = 0$.

5. By Lemma 1 we have $u = x_1^2 x_2 \cdots x_d x_1 \neq 0$. Identities from items 1, 7 of Lemma 1 imply that $x_1^2 abc x_1 = x_1(abc x_1^2) = x_1 bac x_1^2 = x_1^2 bac x_1$ in $N_{3,d}$. The last identity together with item 7 of Lemma 1 imply that $\mathrm{lin}\{u\} = N_{3,d}(31^{d-1})$.

6. It follows from item 3 of Lemma 1. $\triangle$

9 The case of $p = 3$

Notation. For $p = 3$, $r, s, l \geq 0$ determine the set $B_{3^r 1^s}$ of words of multidegree $3^r 1^s$ and the set $B_{3^r 2^s 1^l}$ of words of multidegree $3^r 2^s 1^l$:

$B_{3^{2r} 1^s} = \underline{u}_{2r}\{B_{1^s}|_{x_i \to x_{i+2r},\, i=\overline{1,s}}\} \cup \{\underline{q}_{2r,s,k} | \, k = \overline{1,s}\}$ $(r \geq 0)$,

$B_{3^{2r+1} 1^s} = \underline{u}_{2r} x_{2r+1}^2 x_{2r+2} \{B_{1^s}|_{x_1 \to x_{2r+1},\, x_i \to x_{i+2r+1},\, i=\overline{2,s}}\} \cup \{\underline{q}_{2r+1,s,k} | \, k = \overline{3, s+1}\} \cup \{\underline{q}_{2r+1,s}\}$ $(r \geq 0)$, where

$\underline{q}_{2r,s,k} = \underline{u}_{2r-2} \cdot x_{2r-1}^2 x_{2r}^2 \cdot x_{2r+1} \cdots x_{2r+k} \cdot x_{2r-1} x_{2r} \cdot x_{2r+k+1} \cdots x_{2r+s}$ $(r, s \geq 1$, $k = \overline{1,s})$,

$\underline{q}_{2r+1,s,k} = \underline{u}_{2r} \cdot x_{2r+1}^2 \cdot x_{2r+3} \cdots x_{2r+k} \cdot x_{2r+1} x_{2r+2} \cdot x_{2r+k+1} \cdots x_{2r+s+1}$ $(r \geq 0$, $s \geq 2$, $k = \overline{3, s+1})$,

$\underline{q}_{2r+1,s} = \underline{u}_{2r-2} \cdot x_{2r-1}^2 x_{2r}^2 x_{2r+1}^2 x_{2r-1} x_{2r} x_{2r+1} \cdot x_{2r+2} \cdots x_{2r+s+1}$ $(r \geq 1$, $s \geq 0)$,

$\underline{u}_{2k} = \underline{w}_{12} \cdots \underline{w}_{2k-1,2k}$ $(k \geq 1)$, $\underline{u}_0$ is the empty word,

$\underline{w}_{ij} = x_i^2 x_j^2 x_i x_j$.

Define $B_{3^r 2^s 1^l} = B_{3^r 1^{s+l}}|_{x_i \to x_i^2,\, i=\overline{r+1, r+s}}$.

As an example we point out that $B_{3^0 1^s} = B_{1^s}$, $B_{3^{2r}} = \{\underline{u}_{2r}\}$, $B_{3^{2r+1}} = \{\underline{q}_{2r+1,0}\}$, $B_{3^{2r+1} 1} = \{\underline{u}_{2r} x_{2r+1}^2 x_{2r+2} x_{2r+1},\, \underline{q}_{2r+1,1}\}$.

Theorem 3 *Let $p = 3$.*

1. *A basis for $N_{3,d}(3^r 2^s 1^l)$ is the set $B_{3^r 2^s 1^l}$, where $r, s, l \geq 0$.*
2. *The rest of $\mathcal{N}^d$-homogeneous components of $N_{3,d}$ are equal to zero.*

Remark 3 *For $p = 3$, $r \geq 2$, $s, l \geq 0$ we have $|B_{3^r 2^s 1^l}| = 2^{s+l}$.*

Proof of theorem 3. 1. Consider the homomorphism $\phi : N_{3,d}(3^r 1^{s+l}) \to N_{3,d}(3^r 2^s 1^l)$, defined by

$$\phi(x_i) = \begin{cases} x_i^2 & , \quad r+1 \leq i \leq r+s \\ x_i & , \quad \text{otherwise} \end{cases} .$$

By item 1 of Lemma 1 ϕ is surjective. By Lemma 3 ϕ is injective. Thus, ϕ is an isomorphism of vector spaces. Hence it is sufficient to prove the Theorem for multidegree $3^r 1^s$. The last follows from Lemmas 16, 17 (see below).

2. See item 1 of Lemma 1. $\triangle$

Further for multilinear elements $f_1, f_2 \in K\langle F_d\rangle$, where $\deg(f_1 f_2) = m$, writing $f_1\xi(f_2)$ means that ξ is a substitutional mapping of $\mathcal{M}_{d,m}$ such that the multidegree of $f_1\xi(f_2)$ is equal to 1^m.

Consider $i_1, \dots, i_r \in \{1,2\}$, where $r < d$, and a word u such that

$$\begin{array}{ll} u = x_1 & , \text{ if } r = d-1 \\ u \in \{\underline{e}_{d-r,k} \mid k = \overline{3, d-r}\} & , \text{ if } r < d-1 \end{array} .$$

Denote by $(i_1 i_2 \dots i_r; u)$ the word $w \in B_{1^d}$ which is the result of the following procedure. Let $w_{r+1} = u \in B_{1^{d-r}}$, $w_k = x_{i_k}\xi(w_{k+1}) \in B_{1^{d-k+1}}$ for every $k = \overline{1, r}$. Put $w = w_1$. For short, we will write $(1^{s-1} i_s \dots i_r; u)$ instead of $(1 \dots 1 i_s \dots i_r; u)$ and so on.

Lemma 16 *Let* $r, s \geq 0$. *Then* $\operatorname{lin} B_{3^r 1^s} = N_{3,d}(3^r 1^s)$.

Proof. Let $J_{r,s} = M_{2r+s} \cup \{u x_{2i-1} x_{2i} v,\ u x_{2i} x_{2i-1} v,\ u(x_{2i} a x_{2i-1} + x_{2i-1} a x_{2i}) v,\ u(x_{2i-1} x_{2j-1} x_{2i} b x_{2j} - x_{2i-1} x_{2j-1} x_{2i} x_{2j} b) v \mid u, v \in F_{2r+s},\ a, b \in F^{\#}_{2r+s},\ i, j = \overline{1, r},\ b > x_{2j}\}$ be the subset of $K\langle F_{2r+s}\rangle(1^{2r+s})$.

Consider the homomorphism $\phi : K\langle F_{2r+s}\rangle(1^{2r+s}) \to N_{3,d}(3^r 1^s)$, defined by $\phi(x_{2i-1}) = x_i^2$, $\phi(x_{2i}) = x_i$, $\phi(x_j) = x_{j-r}$, where $i = \overline{1, r}$, $j = \overline{2r+1, 2r+s}$. By item 1 of Lemma 1, ϕ is surjective. Identities $x^2 y^2 x a y = x^2 y^2 x y a$, $x a x^2 + x^2 a x = 0$ of $N_{3,d}$ (see Lemma 1) imply that ϕ induces the epimorphism $\phi_1 : K\langle F_{2r+s}\rangle(1^{2r+s}) / \operatorname{lin}(J_{r,s}) \to N_{3,d}(3^r 1^s)$. By equality (3) we have $N_{3,d}(3^r 1^s) = \operatorname{lin} \phi_1(B(J_{r,s}))$. So in order to prove the statement it is sufficient to prove that

$$\phi_1(B(J_{r,s})) = B_{3^r 1^s}. \tag{8}$$

Note that $B(J_{r,s}) = B(J_{r-1,s+2}) \setminus \overline{J}_{r,s}$ for $r \geq 1$, $s \geq 0$.

For $r = 0$ equality (8) is obvious.

Let $r = 1$. We have $B(J_{1,s}) = B_{1^{s+2}} \setminus \overline{J}_{1,s} = x_1\xi(B_{1^{s+1}}) \cup x_2\xi(B_{1^{s+1}}) \cup \{x_3 \cdots x_k \cdot x_1 x_2 \cdot x_{k+1} \cdots x_{s+2} \mid k = \overline{3, s+2}\} \setminus \overline{J}_{1,s} = x_1\xi(B_{1^{s+1}}) \setminus \overline{J}_{1,s} = x_1 x_2 \xi(B_{1^s}) \cup x_1 x_3 \xi(B_{1^s}) \cup \{x_1 \cdot x_4 \cdots x_k \cdot x_2 x_3 \cdot x_{k+1} \cdots x_{s+2} \mid k = \overline{4, s+2}\} \setminus \overline{J}_{1,s} = x_1 x_3 \xi(B_{1^s}) \cup \{x_1 \cdot x_4 \cdots x_k \cdot x_2 x_3 \cdot x_{k+1} \cdots x_{s+2} \mid k = \overline{4, s+2}\}$. Hence equality (8) holds.

Let $r = 2$. We have $B(J_{2,s}) = B(J_{1,s+2}) \setminus \overline{J}_{2,s} =$ /see above/ $= x_1 x_3 \xi(B_{1^{s+2}}) \cup \{x_1 \cdot x_4 \cdots x_k \cdot x_2 x_3 \cdot x_{k+1} \cdots x_{s+4} \mid k = \overline{4, s+4}\} \setminus \overline{J}_{2,s} = x_1 x_3 \xi(B_{1^{s+2}}) \setminus \overline{J}_{2,s} = x_1 x_3 x_2 \xi(B_{1^{s+1}}) \cup x_1 x_3 x_4 \xi(B_{1^{s+1}}) \cup \{x_1 x_3 \cdot x_5 \cdots x_k \cdot x_2 x_4 \cdot x_{k+1} \cdots x_{s+4} \mid k = \overline{5, s+4}\} \setminus \overline{J}_{2,s} = x_1 x_3 x_2 x_4 \xi(B_{1^s}) \cup x_1 x_3 x_2 x_5 \xi(B_{1^s}) \cup \{x_1 x_3 x_2 \cdot x_6 \cdots x_k \cdot x_4 x_5 \cdot x_{k+1} \cdots x_{s+4} \mid k =$

$\overline{6, s+4}\} \cup \{x_1x_3 \cdot x_5 \cdots x_k \cdot x_2x_4 \cdot x_{k+1} \cdots x_{s+4} |\, k = \overline{5, s+4}\} \setminus \overline{J}_{2,s} = x_1x_3x_2x_4\xi(B_{1^s}) \cup \{x_1x_3 \cdot x_5 \cdots x_k \cdot x_2x_4 \cdot x_{k+1} \cdots x_{s+4} |\, k = \overline{5, s+4}\}$. Thus equality (8) holds.

Let $r = 3$. We have $B(J_{3,s}) = B(J_{2,s+2}) \setminus \overline{J}_{3,s} =$ /see above/ $= x_1x_3x_2x_4\xi(B_{1^{s+2}}) \cup \{x_1x_3 \cdot x_5 \cdots x_k \cdot x_2x_4 \cdot x_{k+1} \cdots x_{s+6} |\, k = \overline{5, s+6}\} \setminus \overline{J}_{3,s} = x_1x_3x_2x_4\xi(B(J_{1,s})) \cup \{x_1x_3 \cdot x_5 \cdot x_2x_4 \cdot x_6 \cdots x_{s+6}\}$. Thus equality (8) is proved to be true.

Let $r \geq 4$. By induction on r prove that

$$B(J_{r,s}) = x_1x_3x_2x_4\xi(B(J_{r-2,s})), \text{ where } r \geq 4. \tag{9}$$

Induction base. Let $r = 4$. We have $B(J_{4,s}) = B(J_{3,s+2}) \setminus \overline{J}_{4,s} =$ /see above/ $= x_1x_3x_2x_4\xi(B(J_{1,s+2})) \cup \{x_1x_3x_5x_2x_4x_6 \cdot x_7 \cdots x_{s+8}\} \setminus \overline{J}_{4,s} = x_1x_3x_2x_4\xi(B(J_{2,s}))$.

Induction step. We have $B(J_{r,s}) = B(J_{r-1,s+2}) \setminus \overline{J}_{r,s} =$ /induction hypothesis/ $= x_1x_3x_2x_4\xi(B(J_{r-3,s+2})) \setminus \overline{J}_{r,s} = x_1x_3x_2x_4\xi(B(J_{r-2,s}))$.

Formula (9) implies that equality (8) is valid. △

Lemma 17 *Let $r, s \geq 0$. Then*

1. *The set $B_{3^{2r}1^s}$ is linearly independent in $N_{3,d}$, where $d = 2r + s$.*
2. *The set $B_{3^{2r+1}1^s}$ is linearly independent in $N_{3,d}$, where $d = 2r + s + 1$.*

Proof. Denote by π_i the homomorphism from Lemma 5. Note that for any $k \geq 1$, $v \in B_{1^k}$ words $x_1x_2\xi(v)$, $x_2x_1\xi(v)$ belong to $B_{1^{k+2}}$. Denote $\pi_1 \cdots \pi_{2r-2}(\underline{u}_{2r-2}) = u$.

1. If $r = 0$, then see Theorem 1. Let $r \geq 1$. For $v \in B_{1^s}$, $k = \overline{1, s}$ we have $\pi_1 \cdots \pi_{2r}(\underline{u}_{2r}\xi(v)) = u(x_{2r-1}x_{2r} - x_{2r}x_{2r-1})\xi(v)$, $\pi_1 \cdots \pi_{2r}(\underline{q}_{2r,s,k}) = u\xi(a - b - c + d)$, where $a = x_3 \cdots x_{k+2} \cdot x_1x_2 \cdot x_{k+3} \cdots x_{s+2} = \underline{e}_{s+2,k+2} \in B_{1^{s+2}}$, $b = x_1 \cdot x_3 \cdots x_{k+2} \cdot x_2 \cdot x_{k+3} \cdots x_{s+2} = (12^k1^{s-k}; x_1) \in B_{1^{s+2}}$, $c = x_2 \cdot x_3 \cdots x_{k+2} \cdot x_1 \cdot x_{k+3} \cdots x_{s+2} = (2^{k+1}1^{s-k}; x_1) \in B_{1^{s+2}}$, $d = x_1x_2 \cdot x_3 \cdots x_{k+2} \cdot x_{k+3} \cdots x_{s+2} = (1^{s+1}; x_1) \in B_{1^{s+2}}$. By above remark, for any $w \in B_{3^{2r}1^s}$ we have $\pi_1 \cdots \pi_{2r}(w) = \sum_i \alpha_{w,i}a_{w,i}$, where $\alpha_{w,i} \in K$, $a_{w,i} \in B_{1^{2r+s}}$. By item 1 of Remark 1, we get that the set $\{\sum_i \alpha_{w,i}a_{w,i} |\, w \in B_{3^{2r}1^s}\}$ is linearly independent in $K\langle F_d\rangle$. So the assumption that $B_{3^{2r}1^s}$ is linearly dependent in $N_{3,d}$ gives that $B_{1^{2r+s}}$ is linearly dependent in $N_{3,d}$ (see Lemma 5), and the last contradicts Theorem 1.

2. Let $v \in B_{1^s}$, $k = \overline{3, s+1}$. Denote $a_v = \pi_1 \cdots \pi_{2r+1}(\underline{u}_{2r}x_{2r+1}^2x_{2r+2}\xi(v))$, $b_k = \pi_1 \cdots \pi_{2r+1}(\underline{q}_{2r+1,s,k})$, $c = \pi_1 \cdots \pi_{2r+1}(\underline{q}_{2r+1,s})$. Let ϕ_1 be the homomorphism from item 4 of Lemma 5. We have that $a_v = u(x_{2r-1}x_{2r} - x_{2r}x_{2r-1})(x_{2r+2}\xi(v) - x_{2r+1}x_{2r+2}\xi(\phi_1(v)))$, $b_k = u(x_{2r-1}x_{2r} - x_{2r}x_{2r-1})(x_{2r+3} \cdots x_{2r+k} \cdot x_{2r+1}x_{2r+2} \cdot x_{2r+k+1} \cdots x_{2r+s+1} - x_{2r+1} \cdot x_{2r+3} \cdots x_{2r+k} \cdot x_{2r+2} \cdot x_{2r+k+1} \cdots x_{2r+s+1}) = u(x_{2r-1}x_{2r} - x_{2r}x_{2r-1})\xi(\underline{e}_{s+1,k} - (12^{k-2}1^{s-k+1}; x_1))$, $c = u(x_{2r-1}x_{2r+1}x_{2r} - x_{2r}x_{2r-1}x_{2r+1} + x_{2r}x_{2r+1}x_{2r-1} - x_{2r+1}x_{2r-1}x_{2r})x_{2r+2} \cdots x_{2r+s+1} = u\xi((121^s; x_1) - (21^{s+1}; x_1) +$

$(2^2 1^s; x_1) - \underline{e}_{s+3,3})$. Above remark and Lemma 14 imply that $a_v, b_k, c \in \operatorname{lin} B_{1^{2r+s+1}}$. Thus $a_v = \sum_i \alpha_{v,i} a_{v,i}$, $b_k = \sum_i \beta_{k,i} b_{k,i}$, $c = \sum_i \gamma_i c_i$, where $\alpha_{v,i}, \beta_{k,i}, \gamma_i \in K$, $a_{v,i}, b_{k,i}, c_i \in B_{1^{2r+s+1}}$. The set $\{a_v, b_k, c \mid v \in B_{1^s},\, k \in \overline{3, s+1}\}$ is linearly independent, because of each set from the class of sets $\{\{a_{v,i}\}, \{b_{k,i}\}, \{c_i\} \mid v \in B_{1^s},\, k \in \overline{3, s+1}\}$ contains an element which does not belong to other sets. Thus the assumption that $B_{3^{2r+1}1^s}$ is linearly dependent in $N_{3,d}$ gives that $B_{1^{2r+s+1}}$ is linearly dependent in $N_{3,d}$ (see Lemma 5), and the last contradicts Theorem 1. $\triangle$

10 Matrix invariants

Let $n \geq 2$. Denote by $M_{n,d}(K) = M_n(K) \oplus \cdots \oplus M_n(K)$ the sum of d copies of the space of $n \times n$ matrices. The general linear group $GL_n(K)$ acts on $M_{n,d}(K)$ by diagonal conjugation: for $g \in GL_n(K)$, $A_i \in M_n(K)$ $(i = \overline{1, d})$ we have $g(A_1, \ldots, A_d) = (gA_1g^{-1}, \ldots, gA_dg^{-1})$. The coordinate ring of the affine space $M_{n,d}(K)$ is the polynomial algebra $K_{n,d} = K[x_{ij}(r) \mid 1 \leq i, j \leq n,\ r = \overline{1, d}]$, where $x_{ij}(r)$ stands for the function such that the image of $(A_1, \ldots, A_d) \in M_{n,d}(K)$ is (i, j)th entry of the matrix A_r. The action of $GL_n(K)$ on $M_{n,d}(K)$ induces the action on $K_{n,d}$: $(g \cdot f)(A) = f(g^{-1}A)$, where $g \in GL_n(K)$, $f \in K_{n,d}$, $A \in M_{n,d}$. Denote by $R_{n,d} = \{f \in K_{n,d} \mid \text{for all } g \in GL_n(K) : gf = f\}$ the matrix algebra of invariants. Let $X_r = (x_{ij}(r))_{1 \leq i,j \leq n}$ be the generic matrices of order n $(r = \overline{1, d})$, and let $\sigma_k(A)$ be the coefficients of the characteristic polynomial of a matrix $A \in M_n(K)$, that is $\det(\lambda E - A) = \lambda^n - \sigma_1(A)\lambda^{n-1} + \cdots + (-1)^n \sigma_n(A)$. The algebra $R_{n,d}$ is generated by all elements of the form $\sigma_k(X_{i_1} \cdots X_{i_s})$ (see [5]). The Procesi–Razmyslov Theorem on the relations in $R_{n,d}$ was extended to the case of a field of an arbitrary characteristic in [14].

The goal of the constructive theory of invariants is to find a minimal (i.e. irreducible) homogeneous system of generators (shortly m.h.s.g.) for the algebra of invariants. A m.h.s.g. for $R_{2,d}$ was determined in [12] for $p = 0$, in [10] for $p > 2$, and in [4] for $p = 2$. In [3] some upper and lower bounds on the highest degree of elements of a m.h.s.g. for $R_{n,d}$ are pointed out for an arbitrary p. In [1] in the case $p = 0$ the cardinality of a m.h.s.g. for $R_{3,d}$ was calculated for $d \leq 10$ on a computer, and was shown a way how such set can be constructed by means of a computer programme. The explicit upper bound on the highest degree of elements of a m.h.s.g. for $R_{3,d}$ is given in [9] (except for the case $p = 3$, $d = 6k + 1$, $k > 0$, where the least upper bound is estimated with error not greater than 1). In this section we point out a m.h.s.g. for $R_{3,d}$ for an arbitrary p, d.

The algebra $R_{n,d}$ possesses natural $\mathcal{N}$- and $\mathcal{N}^d$-gradings by degrees and multide-

grees respectively. Denote by $R^+_{n,d}$ the subalgebra generated by all elements of $R_{n,d}$ of positive degree. An element $r \in R_{n,d}$ is called *decomposable*, if it can be expressed in terms of elements of $R_{n,d}$ of lower degree, that is it belongs to the ideal $(R^+_{n,d})^2$. Clearly, $\{r_i\} \in R_{n,d}$ is a m.h.s.g. if and only if $\{\overline{r}_i\}$ is a basis for $\overline{R}_{n,d} = R_{n,d}/(R^+_{n,d})^2$. If two elements $r_1, r_2 \in R_{n,d}$ are equal modulo the ideal $(R^+_{n,d})^2$, we write $r_1 \equiv r_2$. There is a close connection between decomposability of an element of $R_{n,d}$ and equality to zero of some element of $N_{n,d}$ (see Lemma 18 below). Let $A_{n,d}$ be a K-algebra without unity, generated by the generic matrices $X_1, \ldots, X_d$. The homomorphism of algebras $\Phi : A_{n,d} \to N_{n,d}$, defined by $\Phi(X_i) = x_i$, is defined correctly (see [9]).

Remark 4 *For each $\Delta = (\delta_1, \ldots, \delta_d)$, where $\delta_1 \geq \cdots \geq \delta_d \geq 0$, let $G_\Delta \subset R_{n,d}$ be such a set that its image in $\overline{R}_{n,d}$ is a basis for $\overline{R}_{n,d}(\Delta)$. For any multidegree $\Delta = (\delta_1, \ldots, \delta_d)$ define G_Δ by the following way:*

$$G_\Delta = G_{\delta_{\sigma(1)}, \ldots, \delta_{\sigma(d)}}|_{x_{ij}(r) \to x_{ij}(\sigma(r)),\, i,j=\overline{1,n},\, r=\overline{1,d}},$$

where $\sigma \in S_d$, $\delta_{\sigma(1)} \geq \cdots \geq \delta_{\sigma(d)}$. Then, the set $G = \cup_{\delta_1,\ldots,\delta_d \geq 0} G_\Delta$ is a m.h.s.g. for $R_{n,d}$.

Further, we assume that $n = 3$, unless it is stated otherwise.

Let B_Δ be the basis for $N_{3,d}(\Delta)$ from Proposition 2 and Theorems 2, 3. For $u \in K\langle F_d\rangle^\#$ denote $\mathrm{tr}(u) = \mathrm{tr}(u|_{x_i \to X_i,\, i=\overline{1,d}}) \in R_{3,d}$.

Theorem 4 *For multidegree $\Delta = (\delta_1, \ldots, \delta_d)$, where $\delta_1 \geq \cdots \geq \delta_d$, $d \geq 1$, define $G_\Delta \subset R_{3,d}$:*

1) the case of $p \neq 3$:
if $d \geq 2$ and $\delta_d = 1$, then $G_\Delta = \{\mathrm{tr}(u x_d) |\, u \in B_{(\delta_1,\ldots,\delta_{d-1})}\}$,
if $\Delta = 2^3$, then $G_\Delta = \{\mathrm{tr}(X_1^2 X_2^2 X_3^2)\}$,
if $\Delta = 2^2$, then $G_\Delta = \{\mathrm{tr}(X_1^2 X_2^2)\}$,
if $\Delta = 3^2$, then $G_\Delta = \{\mathrm{tr}(X_1^2 X_2^2 X_1 X_2)\}$,
if $d = 1$, $\Delta = k$, $k = \overline{1,3}$, then $G_\Delta = \{\sigma_k(X_1)\}$,
for others Δ we define $G_\Delta = \emptyset$;

2) the case of $p = 3$:
if $d \geq 2$ and $\delta_d = 1, 2$, then $G_\Delta = \{\mathrm{tr}(u x_d^{\delta_d}) |\, u \in B_{(\delta_1,\ldots,\delta_{d-1})}\}$,
if $\Delta = 3^{2k}$, $k > 0$, or $\Delta = 3^{6k+1}$, $k > 0$, then $G_\Delta = \{\mathrm{tr}(u) |\, u \in B_\Delta\}$,
if $d = 1$, $\Delta = k$, $k = \overline{1,3}$, then $G_\Delta = \{\sigma_k(X_1)\}$,
for others Δ we define $G_\Delta = \emptyset$.

Then, the set G from Remark 4 is a minimal system of generators for $R_{3,d}$.

In order to prove the Theorem we need some statements from [9] and its corollaries:

Lemma 18 *1. Let $H \in A_{3,d-1}$. Then* $\mathrm{tr}(HX_d)$ *is decomposable if and only if* $\Phi(H)=0$ *in* $N_{3,d}$.

2. If $\mathrm{tr}(HX_d^2)\equiv 0$*, where* $H\in A_{3,d-1}$*, then* $\Phi(H)x_d+x_d\Phi(H)=0$ *in* $N_{3,d}$.

3. Let $p=3$*,* $H\in A_{3,d-1}$*. Then* $\mathrm{tr}(HX_d^2)\equiv 0$ *if and only if* $\Phi(H)=0$ *in* $N_{3,d-1}$.

4. If $\mathrm{tr}(u)$ *is indecomposable, where* u *is a word, then there are canonical words* u_i*,* $\mathrm{mdeg}(u)=\mathrm{mdeg}(u_i)$*, and* $\alpha_i\in K$*, such that* $\mathrm{tr}(u)\equiv\sum\alpha_i\mathrm{tr}(u_i)$.

5. We have $\sigma_2(UV)\equiv\mathrm{tr}(U^2V^2)$*, where* $U,V\in A_{3,d}$.

6. Elements $\sigma_2(X_1)$*,* $\det(X_1)$ *are indecomposable.*

7. If $p\neq 3$*, then* $\mathrm{tr}(X_1^2X_2^2X_3^2)+\mathrm{tr}(X_1^2X_3^2X_2^2)\equiv 0$*. For any* p*, the element* $\mathrm{tr}(X_1^2X_2^2X_3^2)$ *is indecomposable.*

8. Let $p=3$*,* $u_i\in F_d$ *are words,* $\mathrm{mdeg}(u_i)=\Delta$*. Then* $\sum_i\alpha_i\mathrm{tr}(u_i)\equiv 0$ *if and only if* $\sum_i\alpha_iu_i=0$ *is a consequence of the system of identities* $\mathcal{S}_\Delta$ *and identities* $uv=vu$*, where* $u,v\in F_d^{\#}$ *and* $\mathrm{mdeg}(uv)=\Delta$.

9. For $u,v\in F_d$*, where* $\mathrm{mdeg}(uv)=3^{2k}$*,* $k>0$*, or* $\mathrm{mdeg}(uv)=3^{6k+1}$*,* $k>0$*, we have* $uv=vu$ *in* $N_{3,d}$.

10. Let D *be the explicit upper bound on degrees of elements of a m.h.s.g. for* $R_{3,d}$*, where* $d\geq 2$*. Then*

if $p=0$ *or* $p>3$*, then* $D=6$*;*

if $p=2$*, then* $D=\left\{\begin{array}{ccl} d+2 & , & d\geq 4\\ 6 & , & d=2,3\end{array}\right.$*;*

if $p=3$ *and* $d=6k+r$*, where* $r\in\{3,5\}$*,* $k\geq 0$*, then* $D=3d-1$.

Proof. All items except for 3, 7 are proven in [9].

3. If $\mathrm{tr}(HX_d^2)\equiv 0$, then $\Phi(H)x_d+x_d\Phi(H)=0$ in $N_{3,d}$ (see item 2). By item 4 of Lemma 5 we have $2\Phi(H)=0$ in $N_{3,d}$. The converse follows from item 1.

7. Let $p\neq 3$. The identity $x_1^2x_2x_3^2=0$ in $N_{3,d}$ (Lemma 1 item 4) implies $\mathrm{tr}(X_1^2X_2X_3^2X_2)\equiv 0$ (see item 1). On the other hand, the identity $x_2x_3^2x_2=-x_2^2x_3^2-x_3^2x_2^2$ in $N_{3,d}$ (see identity (1)) implies $\mathrm{tr}(X_1^2X_2X_3^2X_2)\equiv-\mathrm{tr}(X_1^2X_2^2X_3^2)-\mathrm{tr}(X_1^2X_3^2X_2^2)$ (see item 1). The claim is proved.

Assuming $\mathrm{tr}(X_1^2X_2^2X_3^2)\equiv 0$, we get $x_1^2x_2^2x_3+x_3x_1^2x_2^2=0$ in $N_{3,d}$ by item 2. Thus $x_1^2x_2^2x_1=-x_1x_1^2x_2^2=0$ in $N_{3,d}$; that is a contradiction to item 2 of Lemma 1. $\triangle$

Proof of theorem 4. By items 4, 5 of Lemma 18, we have that $R_{3,d}$ is generated by $\{\sigma_2(X_i),\det(X_i),\mathrm{tr}(u)|\,u\in F_d^{\#}$ is a canonical word, $i=\overline{1,d}\}$.

Let $p\neq 3$. The claim follows from items 1, 6, 7 and 10 of Lemma 18.

Let $p=3$. The case of $\delta_d=1,2$ follows from items 1, 3 of Lemma 18. The case of $\Delta=3^d$ follows from items 8, 9, 10 of Lemma 18. $\triangle$

ACKNOWLEDGEMENTS

The author is supported by RFFI (grant 04.01.00489). The author is grateful to the referee whose comments considerably improved the paper.

References

[1] S. Abeasis, M. Pittaluga, *On a minimal set of generators for the invariants of* 3×3 *matrices*, Comm. Algebra 17(1989), 487–499.

[2] L.A.Bokut', G.P. Kukin, *Algorithmic and combinatorial algebra*, Mathematics and its applications (Kluwer Academic Publishers), v. 255, 1993.

[3] M. Domokos, *Finite generating system of matrix invariants*, Math.Pannon. 13(2002), N2, 175–181.

[4] M. Domokos, S.G. Kuzmin, A.N. Zubkov, *Rings of matrix invariants in positive characteristic*, J. Pure Appl. Algebra 176(2002), 61–80.

[5] S. Donkin, *Invariants of several matrices*, Invent. Math. 110(1992), 389–401.

[6] G.Higman, *On a conjecture of Nagata*, Math. Proc. Cambridge Philos. Soc. 52(1956), 1–4.

[7] A.A.Klein, *Bounds for indices of nilpotency and nility*, Arch. Math. (Basel) 76(2000), 6–10.

[8] E.N. Kuzmin, *On the Nagata–Higman theorem*, in: Mathematical Structures — Computational Mathematics — Mathematical Modeling, Proceedings Dedicated to the 60th Birthday of Academician L.Iliev, Sofia, 1975, 101–107 (Russian).

[9] A.A. Lopatin, *The algebra of invariants of* 3×3 *matrices over a field of arbitrary characteristic*, Comm. Algebra 32(2004), N7, 2863–2883.

[10] C. Procesi, *Computing with* 2×2 *matrices*, J. Algebra 87(1984), 342–359.

[11] Yu.P. Razmyslov, *Identities of algebras and their representations*, Translations of Mathematical Monographs, 138, American Math. Soc., Providence, RI, 1994.

[12] K.S. Sibirskii, *Algebraic invariants for a set of matrices*, Sibirsk. Mat. Zh. 9(1968), N1, 152–164 (Russian).

[13] M.R. Vaughan–Lee, *An algorithm for computing graded algebras*, J. Symbolic Comput., 16(1993), 345–354.

[14] A.N. Zubkov, *On a generalization of the Razmyslov–Procesi theorem*, Algebra i Logika 35(1996), N4, 433–457 (Russian).